CYBERBEZPIECZEŃSTWO W POKOWIDOWYM ŚWIECIE. GŁOS EKSPERTÓW

Jakie wyzwania i zagrożenia w obszarze cyberbezpieczeństwa staną przed polskim biznesem oraz administracją w 2021 roku? Jak likwidacja Ministerstwa Cyfryzacji wpłynie na współpracę biznes-administracja publiczna? O opinie zapytaliśmy ekspertów.

Pandemia Koronawirusa, która ogarnęła cały świat doprowadziła do głębokich zmian w pracy instytucji publicznych i prywatnych. Ogromna ilość pracowników wykonywała swoje obowiązki z domu, co zmieniło świat biznesu, ale było też dużym wyzwaniem dla cyberbezpieczeństwa. Phishing oparty o wiadomości związane z COVID-19 sprawiał problemy użytkownikom, tak samo jak ataki ransomware stanowiły zmartwieniem dla administratorów sieci. O dokonanie podsumowania, a także zdiagnozowanie trendów oraz postawienie prognoz na 2021 rok poprosiliśmy ekspertów:

- Izabelę Albrycht, prezes Instytutu Kościuszki oraz przewodniczącą Komitetu Organizacyjnego Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC;
- Martina Mellora, szefa Ericssona w Polsce;
- Dariusza Piotrowskiego, dyrektora generalnego Dell Technologies Polska;
- Rafała Jaczyńskiego, Regional Cyber Security Officer CEE & Nordics Huawei.

Jak Pani/Pan ocenia funkcjonowanie polskiego biznesu po przejściu na tryb zdalny podczas tegorocznej pandemii?

„Niestety fakt, o którym alarmowaliśmy od wielu lat, a więc niski poziom i niewystarczająca szybkość wdrażania bezpiecznych rozwiązań cyfrowych w polskiej gospodarce, odbiły się na tym czego byliśmy świadkami w zderzeniu z pierwszą falą pandemii w marcu. Wtedy głównym problemem dla polskich przedsiębiorstw jak i instytucji stała się nie tylko walka z czasem o powrót do ciągłości działania (*business continuity*) dzięki wdrożeniu narzędzi cyfrowych, ale także znalezienie budżetu umożliwiającego ich zakup i wdrożenie. Przy drugiej fali pandemii widać już jednak poprawę w zakresie zdolności przedsiębiorstw i administracji publicznej do pracy zdalnej i sprawniejsze świadczenie usług cyfrowych dla klientów” - podkreśla Izabela Albrycht. Prezes Instytutu Kościuszki wtóruje Dariusz Piotrkowski, twierdząc, że „organizacje, które do tej pory wstrzymywały się z technologicznymi inwestycjami zrozumiały, że digitalizacja to już nie tylko kwestia budowania przewagi konkurencyjnej, ale zwykłego funkcjonowania; w wielu organizacjach w pośpiechu wdrażano kluczowe procesy czy kupowano laptopy dla pracowników, by utrzymać ciągłość biznesową. Jak pokazało nasze ostatnie badanie Digital Transformation Index, przeprowadzane w trakcie pandemii, celem aż 81% polskich firm jest teraz priorytetyzacja programów cyfrowej transformacji, dlatego z pewnością będziemy obserwować zwiększoną mobilizację w stronę takich inwestycji jeszcze przez dłuższy czas”.

Na pozytywne skutki pandemii w obszarze cyfryzacji wskazuje Rafał Jaczyński z Huawei. Jego zdaniem

„poza oczywistymi negatywnymi skutkami pandemii, warto zauważyć ten jeden pozytywny: błyskawiczne przyspieszenie procesów transformacji cyfrowej przedsiębiorstw i instytucji publicznych. Mówi się, że COVID jako Wielki Cyfryzator w kilka miesięcy zrealizował inicjatywy cyfryzacji zaplanowane na dekadę".

Z kolei Martin Mellor zwraca uwagę na rolę sektora telekomunikacyjnego. „Pandemia naprawdę pokazała, że sieci komórkowe stanowią infrastrukturę krytyczną dla poszczególnych państw. Dzięki nim firmy, rodziny i grupy przyjaciół utrzymywały łączność przez cały ten czas. Jeśli spojrzeć na statystyki ruchu w sieciach, to możemy zauważyć, że ruch głosowy wzrósł o 50%, zaś transmisja danych zwiększyła się o 20%" - twierdzi szef Erickssona.

Czytaj też: The best of CyberDefence24 w roku 2020

Jakie wyzwania oraz zagrożenia w obszarze cyberbezpieczeństwa staną przed polskim biznesem i administracją w 2021 roku?

„Od czasu pandemii obserwujemy zwiększoną aktywność ataków i to nie tylko na organizacje biznesowe, ale także na szkoły, uczelnie, urzędy. Do tego dochodzi fakt, że z roku na rok drastycznie rośnie liczba danych, które przechowujemy i przetwarzamy - badanie Data Protection Global Index mówi, że w tym roku organizacje zarządzają średnio nawet o 40% większą liczbą danych niż rok wcześniej, więc rozwiązania muszą być elastyczne, skalowalne i przede wszystkim - odporne na ataki" - podkreśla Dariusz Piotrowski, dyrektor generalny Dell Technologies Polska.

„Największym wyzwaniem staje się też zmiana świadomościowa zarządów firm wszelkiej wielkości, dotycząca tego, że pandemii towarzyszy także pandemia cyberzagrożeń. Ich liczba od marca br. znacznie wzrosła i aktualnie rośnie dosłownie z dnia na dzień. A zatem zapewnienie cyberbezpieczeństwa staje się działaniem numerem jeden, umożliwiającym niezakłócone funkcjonowanie firmy. W analizie ryzyka, wydatki na cyberbezpieczeństwo w firmach powinny mieć podobny poziom wskaźnika jak utrata płynności finansowej" - wskazuje prezes Instytutu Kościuszki Izabela Albrycht.

Szef Ericssona w Polsce zauważa, „że każda generacja w technologii wprowadza ulepszenia w zakresie bezpieczeństwa i 5G, z szeregiem nowych mechanizmów bezpieczeństwa, jak na przykład szyfrowanie typu end-to-end z konfiguracją IMSI, nie różni się pod tym względem od poprzednich. Ze względu na fakt, że 5G będzie wykorzystywane przez prawie wszystkie polskie przedsiębiorstwa, ważne jest, aby miały one pewność, że ich prawa własności intelektualnej są bezpieczne w sieci".

Rafał Jaczyński, z Huawei nawiązuje do nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa. W jego opinii „według zapowiedzi ministra Zagórskiego, w styczniu możemy spodziewać się zaprezentowania nowej wersji ustawy o Krajowym Systemie Cyberbezpieczeństwa. W swoim poprzednim wydaniu z września br. projekt zawierał szereg zapisów, które mocno godziły w interesy operatorów telekomunikacyjnych, a jednocześnie w żaden sposób nie przyczyniały się do zwiększenia poziomu cyberbezpieczeństwa. Mam nadzieję, że osoby odpowiedzialne za KSC dokładnie przeanalizowały liczne głosy sprzeciwu, jakie spłynęły do nich z rynku oraz z organów takich jak Ministerstwo Rozwoju czy Ministerstwo Sprawiedliwości, i wezmą je sobie do serca".

Czytaj też: Rok 2020 z (cyber)perspektywy. Przełomowy czy marginalny?

Jak likwidacja Ministerstwa Cyfryzacji wpłynie na współpracę biznes-administracja

publiczna?

Rafał Jaczyński jest zaniepokojony likwidacją resortu cyfryzacji. „Ze zaniepokojeniem patrzyłem na likwidację tej młodej instytucji, która powstała m.in. po to, by przy użyciu nowych technologii modernizować polską administrację publiczną, a tym samym ułatwiać życie Polakom i polskim przedsiębiorcom. Polski sektor ICT/IT ma prawo czuć się osierocony, a polski podatnik zaskoczony, że sytuując się pod względem korzystania z urzędowych e-usług wciąż poniżej średniej w Unii Europejskiej" - podkreśla przedstawiciel Huawei.

Optymistycznie do sprawy podchodzi Izabela Albrycht, która pisze: „nazwałabym ten proces raczej transformacją ministerstwa cyfryzacji i jego zasobów w ramach struktury KPRM. Liczę na to, że takie usytuowanie tego tematu w ramach administracji rządowej ułatwi bardziej holistyczne spojrzenie na potrzebę takiej współpracy i sprawniejsze jej przeprowadzenie. Ta współpraca w wielu miejscach jest realizowana, ale w wielu także musi przyspieszyć. To często bardziej sektor prywatny jest tego świadomy, organizując się >oddolnie<". Również Dariusz Piotrowski nie widzi większych zmian we współpracy z resortem. „Z naszego punktu widzenia zmian nie zauważamy, ponieważ w ramach realizacji naszych programów pracujemy dokładnie z tymi samymi zespołami. Projekty, które zapoczątkowaliśmy z Ministerstwem Cyfryzacji są kontynuowane w niezmienionej formie. Dotyczy to np. realizacji Programu Współpracy w Cyberbezpieczeństwie (PWCyber). Jego celem jest zwiększenie poziomu cyberbepieczeństwa polskich firm i instytucji poprzez działania edukacyjne dla przedsiębiorców z ekspertami Dell Technologies" - podkreśla. Piotrkowskiemu wtóruje Martin Mellor, który twierdzi, że „ze swojej perspektywy mogę jednak zauważyć, że nie miało to dotychczas wpływu na współpracę publiczno-prywatną. Jednym z przykładów takiej współpracy jest program PWCyber, który jest przykładem inicjatywy podjętej przez rząd i dostawcami technologii informacyjno-komunikacyjnych na rzecz współpracy w zakresie cyberbezpieczeństwa".

Pełne wypowiedzi ekspertów znajdują się poniżej:

- Izabela Albrycht, prezes Instytutu Kościuszki oraz przewodnicząca Komitetu Organizacyjnego Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC;
- Martin Mellor, szef Ericssona w Polsce;
- Dariusz Piotrowski, dyrektor generalny Dell Technologies Polska;
- Rafał Jaczyński, Regional Cyber Security Officer CEE & Nordics Huawei.

Czytaj też: (Cyber)wyzwania dla Wojska Polskiego oczami przedstawicieli armii