Ireneusz Piecuch, Partner Zarządzający w Kancelarii IMP

Od sierpnia do sierpnia

Czy jesteśmy już bezpieczni?

Rok temu weszły w życie przepisy ustawy ustanawiającej Krajowy System Cyberbezpieczeństwa. Na początku sierpnia ukazał się natomiast, przeznaczony do konsultacji, projekt Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, a Unia Europejska uchwaliła kolejne ważne rozporządzenie. Czy wnoszą one coś nowego z punktu widzenia polskich przedsiębiorstw?

fot. Pixabay.com

Rok temu weszły w życie przepisy ustawy ustanawiającej Krajowy System Cyberbezpieczeństwa. Po raz pierwszy w polskim ustawodawstwie, doczekaliśmy się kompleksowej regulacji obejmującej całe sektory polskiej gospodarki, żeby wspomnieć tu tylko o sektorze paliwowo-energetycznym, sektorze transportu, bankowości, ochronie zdrowia, czy też sektorze infrastruktury cyfrowej. Regulacji, będącej implementacją dyrektywy NIS z 2016 r., pierwszego poważnego kroku na drodze do zbudowania jednolitego, europejskiego systemu ochrony przed cyberzagrożeniami. Pisałem o tym szerzej w numerze 4 „Nowej Energii" w 2018 r.

Od tego czasu pojawiło się kilka rozporządzeń wykonawczych (niektóre wzbudzając mocne kontrowersje). Tempo wdrożenia ustawy wydaje się jednak dalekie od zakładanego. Do maja br., a więc po ponad pół roku od wejścia w życie ustawy, mówiło się o około 70 wydanych decyzjach uznających poszczególne spółki za spółki świadczące usługi krytyczne (na około 500 przedsiębiorstw, które taką decyzję powinny otrzymać).

Na początku sierpnia ukazał się natomiast, przeznaczony do konsultacji, projekt Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 (dalej przywoływanej jako „Strategia"), który w zamyśle ma zastąpić obowiązujące obecnie Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022. Jako, że dokument ten powstawał w okresie wdrażania ustawy o KSC, powinien on już odzwierciedlać pierwsze doświadczenia wynikające z tego procesu, jak również zmiany w ustawodawstwie europejskim, do których doszło w br. Czy tak jest w istocie?

Wizja i Cele

Strategia jak to strategia, bez wizji ani rusz. I tu, bez zdziwienia (przynajmniej bez zdziwienia wszystkich związanych z tematem), możemy przeczytać, że pomyślny rozwój naszego kraju jest związany ze „sprawnym i bezpiecznym działaniem systemów informatycznych i środków komunikacji elektronicznej". Stąd już tylko krok do stwierdzenia, że rząd nie poprzestanie jedynie na wdrożeniu ustawy o KSC, ale zamierza systematycznie wzmacniać i rozwijać ów system. To jasny sygnał dla wszystkich tych, którzy ustawili ustawę o KSC w szeregu innych ustaw związanych z zapewnieniem zgodności regulacyjnej. KSC w obecnym kształcie to dopiero początek. Stąd rozwój tego systemu został wymieniony jako cel szczegółowy Strategii nr 1.

Na kolejnych miejscach znalazło się „stymulowanie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności skutecznego zapobiegania incydentom". I ten cel nie powinien budzić wątpliwości, zwłaszcza jeśli wziąć pod uwagę to, że od wystąpienia incydentu do jego wykrycia, wedle różnych opracowań mija od 50 do 90 dni. Cel 3 wiąże się ze zwiększeniem potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni. Cel 4 odwołuje się do jakże istotnej kwestii budowania świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa. Natomiast cel 5 deklaruje odgrywanie aktywnej roli na arenie międzynarodowej.

Z punktu widzenia przedsiębiorstw, z pewnością warto się bliżej przyjrzeć celom 1, 2 oraz 3.

Regulacje Sektorowe na Celowniku

Tak jak już wspomniałem, uchwalenie KSC trzeba traktować jako początek, a nie koniec prac legislacyjnych w obszarze cyberbezpieczeństwa. Strategia zakłada, że Minister Cyfryzacji, we współpracy z innymi resortami, dokona przeglądu regulacji sektorowych.

Tu i ówdzie pojawiły się głosy, że to tak naprawdę sprawa dla informatyków. Szefowie spółek, z którymi rozmawiałem kiwają ze zrozumieniem głowami, wspominając, że może uda im się zwiększyć nakłady w tej mierze ... w przyszłorocznym budżecie. Zastrzegają jednak szybko, że może być różnie, bo projekty nastawione na wzrost przychodu (lub ograniczenie kosztów) mają absolutny priorytet. Słucham tego wszystkiego i myślę, że warto byłoby zacząć od początku.

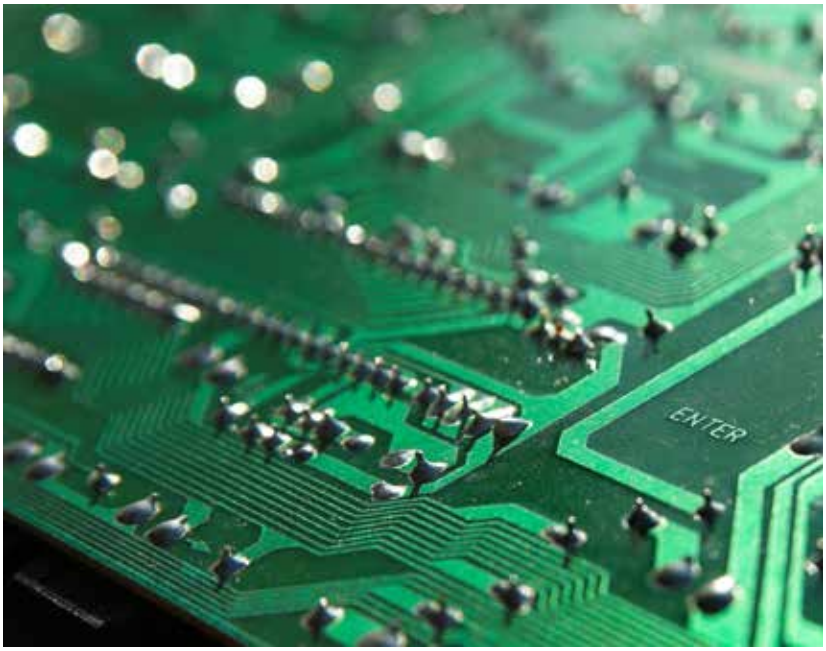
Jak to jest z tymi cyberzagrożeniami?

McAfee, amerykańska firma specjalizująca się w zabezpieczeniach systemów komputerowych ocenia, że działalność cyberprzestępców kosztowała globalną gospodarkę tylko w 2017 r. około 600 mld dolarów - prawie 0.8% światowego GDP. W miejsce nastoletnich hackerów włamujących się do cudzych systemów dla samej satysfakcji złamania zabezpieczeń, pojawiły się zorganizowane grupy przestępcze, ba całe armie zdyscyplinowanych, świetnie wykształconych informatyków, działających nierzadko pod auspicjami rządowymi. Skala tej przestępczości ustępuje jeszcze korupcji oraz narkobiznesowi, ale już wkrótce kolejność ta może się zmienić (rok do roku odnotowuje się wzrost dwucyfrowy). Cyberprzestępcy są bowiem w czołówce „przedsiębiorców" korzystających z najnowszych rozwiązań cyfrowych. Ba, wydają na rozwój, badania i inwestycje dziesięciokrotnie więcej niż przedsiębiorstwa na zabezpieczenia w tej mierze (specjaliści mówią o nakładach rzędu biliona dolarów).

Płatności cyfrowe w znakomity sposób pozwoliły im na minimalizację ryzyka związanego z pobieraniem haraczu za odblokowanie zainfekowanych złośliwym oprogramowaniem serwerów, a chmura obliczeniowa na wykorzystywanie nielimitowanych zasobów informatycznych. Setki milionów różnego rodzaju urządzeń przyłączanych do sieci w ramach internetu rze-

czy (IOT), pozbawionych jakiejkolwiek ochrony przed przejęciem kontroli, stanowią niewyczerpane źródło urządzeń wykorzystywanych do ataków DDoS. Ciemna strona internetu tzw. Dark Net, zapewnia możliwość handlu skradzionymi danymi na niespotykaną wręcz skalę. Prawdziwe przestępcze Eldorado - i do tego cyfrowe. I jeszcze jedno udogodnienie: niska wykrywalność i jeszcze niższa skuteczność ścigania. Przestępczość cyfrowa to biznes z definicji globalny. Nie zna granic, czy problemów językowych, a jego ofiarą może paść każdy... z wyjątkiem mieszkańców obszarów wykluczonych cyfrowo (kto wie, być może likwidacja wszystkich tych obszarów nie jest do końca dobrym pomysłem?).

Te 600 mld strat to głównie wykradziona własność intelektualna, nadużycia finansowe, okup uzyskiwany od przedsiębiorców za odblokowanie ich systemów informatycznych, pieniądze uzyskane z handlu informacjami na temat kard kredytowych, czy też innych przydatnych danych. Po stronie poszkodowanych mogą być osoby fizyczne, firmy, rządy i całe społeczeństwa. Centralny Bank Bangladeszu stracił ponad 80 mln dolarów, a był o krok od utraty mld. Na drodze przestępcom nie stanął jednak zespół specjalistów od zabezpieczeń, a urzędnik bankowy, który zwrócił uwagę na nieścisłość w poleceniu przelewu. Aramco - jeden z najbogatszych koncernów świata utracił mln dolarów, po tym jak większość stacji roboczych tego koncertów została zainfekowana, a zawarte na nich dane utracone. Irański projekt jądrowy został skutecznie opóźniony na lata po ataku wirusa Stuxnet. Czy przykład z ostatniego roku - firma Equifax i wyciek ponad 145 mln danych klientów tej firmy. Spadek wartości w kwartale następującym po wycieku - 27%. Kwota wydana na rozbudowę systemów zabezpieczeń w ciągu ostatnich 12 miesięcy - ponad 200 mln dolarów. Taką listę można by mnożyć w nieskończoność, mimo że jak podają źródła brytyjskie, jedynie 13% incydentów związanych z cyberatakami jest ujawnianych przez zaatakowane firmy.



fot: Pixabay.com

To dzisiaj. A jutro?

Mamy już udokumentowane przykłady możliwości przejęcia kontroli nad urządzeniami wspomagającymi pracę serca (swego czasu, ówczesny wiceprezydent USA, Dick Chenney, przeszedł dodatkowy zabieg mający na celu wyłączenie modułu zdalnego sterowania w wszczepionym mu urządzeniu). Mamy przykłady zdalnego przejęcie kontroli nad systemem hamulcowym samochodu (większość produkowanych obecnie samochodów ma możliwość zdalnej współpracy z pokładowym systemem komputerowym). Wiemy o dokonanej z sukcesem penetracji infrastruktury krytycznej i wykorzystania zasobów informatycznych wspomagających jej pracę do ... kopania bitcoinów. Internet rzeczy, e-zdrowie, sztuczna inteligencja niosą z sobą nowe obietnice, ale też nowe zagrożenia. Także i w tej mierze, cyberprzestępcy zdają się być o krok przed nami.

John Chambers, wieloletni szef CISCO powiedział, że firmy dzielą się na dwie kategorie. Te, które zostały zhakowane i wiedzą czym to smakuje oraz te które zostały zhakowane, ale jeszcze o tym nie wiedzą. Ustawa wprowadzająca Krajowy System Cyberbezpieczeństwa ma mnóstwo mankamentów. Nadmiernie zbiurokratyzowany i rozproszony system organów ochrony, brak adekwatnego systemu finansowania, niejasno sformułowane obowiązki firm, możliwość daleko idącej ingerencji ze strony organów etc., etc. Niektórzy, podbudowani przykładem RODO, dodają też do tej listy zbyt niskie kary, choć osobiście nie zgadzam się z tym poglądem. Mimo tych wszystkich mankamentów, ustawa ta jest jednak niewątpliwie krokiem we właściwą stronę. Globalny wymiar zagrożeń, wskazuje bowiem na to, że żadne przedsiębiorstwo samodzielnie (nawet tak potężne jak Aramco), nie jest w stanie sobie z nim poradzić. Transformacja cyfrowa jest drogą jednokierunkową. I nawet z naszym zamiłowaniem do opóźnień, będziemy musieli nią podążyć. Zapewnienie możliwości bezpiecznego korzystanie z tej drogi w żadnym razie jednak nie powinno być traktowane wyłącznie w kategorii kosztu, ale raczej jako warunek konieczny dla rozpoczęcia tej podróży. □