2020 POD ZNAKIEM CHMURY, SZTUCZNEJ INTELIGENCJI I WINDOWS 7? PROGNOZA EKSPERTÓW

Sztuczna inteligencja, coraz większa liczba podłączonych urządzeń do Internetu, rosnąca rola chmury oraz kończące się wsparcie dla Windowsa 7 to główne wyzwania cyberbezpieczeństwa w 2020 roku - prognozują eksperci. Będzie to również czas zmian organizacyjnych i prawnych, na które Polska nie jest odpowiednio przygotowana.

Ewa Wernerowicz – prezes Vivus Finance

Zdecydowanie największym zagrożeniem dla cyberbezpieczeństwa i bezpieczeństwa informacji są i pozostaną pracownicy. Mimo technicznie dobrej infrastruktury do większości cyberataków – a według Kaspersky Lab ponad połowa przedsiębiorstw w Europie padała ich celem w 2018 roku – dochodzi do nich z powodu niedopatrzeń lub niestosowania się do wewnętrznej polityki bezpieczeństwa przez pracowników przedsiębiorstwa będącego celem ataku. Moim zdaniem trendem nie będzie, a przynajmniej nie powinno być dalsze umacnianie infrastruktury – która już teraz, jeśli odpowiednio zarządzana, jest trudna do sforsowania przez potencjalnych hakerów. Trendem będzie edukacja pracowników, którzy często nie rozumieją dlaczego nie powinni np. korzystać w firmie z prywatnej poczty czy używać pendrive'ów. Obawiam się, że biznes poświęca zbyt wiele czasu na budowę polityk bezpieczeństwa, a zbyt mało na tłumaczenie ich w sposób który sprawi, że pracownicy przestaną myśleć, że polityki te mają na celu tylko kontrolowanie ich i utrudnianie im pracy. Czujność użytkownika systemu uśpić jest łatwiej niż zmagać się z przełamywaniem, nierzadko zaawansowanych, zabezpieczeń IT.

Ireneusz Piecuch - Partner Zarządzający, Kancelaria IMP

„Rok 2020 nie będzie rokiem przełomu. Eksperci w dalszym ciągu podkreślać będą wagę cyberbezpieczeństwa a prezesi dużych spółek, jak to usłyszałem na jednym z paneli, będą wspierać nakłady na ochronę przed cyberatakami …w miarę swoich możliwości budżetowych. Cyberprzestępcy dalej zatem doskonalić będą swoje arsenały korzystając z takich udogodnień jak lawinowy wzrost urządzeń podłączanych do sieci (IOT) czy sztuczna inteligencja (AI) a ich nakłady pozostaną wielokrotnie większe od tych przeznaczanych na zwiększenie odporności firm przed atakami i zapewnienie ciągłości działania. Niestety wdrożenie Dyrektywy NIS i postanowień ustawy o Krajowym Systemie Cyberbezpieczeństwa postępuje niezmiernie powoli i trudno spodziewać się, że do końca roku zamknie się proces wydawania decyzji w zakresie uznania grupy około 500 polskich przedsiębiorstw za operatorów usługi kluczowej.

Jak wynika z nowej Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej w roku 2020 w dalszym ciągu brakować będzie systemu teleinformatycznego wspierającego współpracę podmiotów tworzących KSC (ma zostać uruchomiony dopiero w 2021 roku). Zakładam też, że dążąc do

zachowania zbilansowanego budżetu państwa, niewiele miejsca zostanie w nim poświęcone ustanowieniu finansowych podstaw dla budowania cyberbezpieczeństwa państwa. Po wielu zapowiedziach w tej mierze należy się za to spodziewać kolejnej regulacji, tym razem zawierającej wytyczne (bo raczej nie standardy) w zakresie cyberbezpieczeństwa sieci 5G. Nie będzie to praca łatwa, bo wskazanie dlaczego produkty jednego producenta są bezpieczne a drugiego nie powinno się odwoływać wyłącznie do ich specyfikacji technicznej, a w takiej sytuacji nie trudno o niespodziankę. W tej sytuacji, ekscytować będziemy się głównie karami nakładanymi przez UODO, które zapewne dość często (tak jak było to w przypadku kary nałożonej na firmę Morele) nawiązywać będą do oceny działań podjętych w zakresie właściwego zabezpieczenia dostępu do przetwarzanych informacji. Kolejnymi zmasowanymi atakami DDoS wykorzystujący idealną mieszankę ignorancji, pogoni za niską ceną i podłączaniem do sieci wszystkiego co tylko się da. No i oczywiście phishingiem który od form prymitywnych podróbek przechodzi do świetnie profilowanych i zindywidualizowanych przekazów. Innymi słowy rok 2020 niczym specjalnie nas nie zaskoczy.

Michał Jaworski - Dyrektor Strategii Technologicznej w Microsoft

Jeśli przyjmiemy, że w cyberprzestrzeni ma miejsce niewypowiedziana i ciągła wojna to warto pamiętać, że wprawdzie bitwy wygrywa się dzięki odwadze żołnierzy, ich wyszkoleniu i dostępnej technice, ale wojny wygrywa się organizacją. Takie podejście jest prawdziwe na poziomie całego państwa, jak i dla małego i średniego przedsiębiorstwa. W triadzie uwarunkowań prawnych, technicznych i organizacyjnych cyberbezpieczeństwa to ostatnie będzie stanowiło w 2020 największe wyzwanie, ponieważ często będzie oznaczało ogromną zmianę w stosunku do niedawnej nawet przeszłości. Zmiany będą również wymuszane przez prawo i doświadczenia wynikające z dotychczasowego jego stosowania (np. uksc, PSD2, ale także decyzje i kary nakładane przez Prezesa UODO). W równie wielkim stopniu sposób funkcjonowania naszych klientów, dostawców i pracowników nakazuje poważne przeanalizowanie tematu. Czyli choćby wprowadzenie zasad zerowego zaufania (Zero Trust) czy Założenie Naruszenia (Assume Breach) w wewnętrznych sieciach. Czyli konieczność wykorzystania zewnętrznych usług cyberbezpieczeństwa, w tym w szczególności usług chmurowych i odpowiedniej relacji biznesowej z dostawcami, bo samodzielnie nikt już nie jest w stanie się dzisiaj obronić. Czyli sprawa kadr – specjalistów od cybersec jest niewielu, ich wynagrodzenie jest wysokie, a popyt na usługi duży. Szansa na zbudowanie własnego, stabilnego zespołu maleje – jak uzyskać więcej mając mniej do dyspozycji. Dopiero teraz sięgamy do technologii, gdzie najciekawsze rozwiązania 2020 będą związane z wykorzystaniem AI, a przez cały rok będziemy się zastanawiali w jaki sposób coraz lepiej widoczne na horyzoncie quantum computing odmieni cyberbezpieczeństwo. Zanim jednak zanurzymy się w przyszłości warto użyć wszystkich narzędzi jakie są na rynku. Btw, ostateczna data wstrzymania jakiegokolwiek suportu dla Windows 7 mija w połowie stycznia 2020 – co zrobiłeś w tej sprawie, drogi Czytelniku?

Rafał Magryś - wiceprezes Exatel

Rynek usług chmurowych jest jednym z najszybciej rosnących segmentów rynku IT w Polsce z przyrostem na poziomie 26-30% rok do roku. To powoduje, że staje się też kuszącym obszarem działań cyberprzestępców. 2020 będzie rokiem zwiększonych ataków na zasoby w chmurze. Będziemy również obserwować stały wzrost ataków DDoS - z roku na rok rośnie ich wolumen oraz częstotliwość. Szczególnie ze względu na nikłe zapieczenie urządzeń podłączanych do sieci takich jak kamerki, lodówki, zabawki dziecięce czy rozwiązań typu smart home. Zmianie ulegnie również cel ataków. Cyberataki coraz mocniej zaczną dotykać instytucji samorządowych. Mieliśmy tego przykłady już w tym roku np. w Tarnowie czy niedawno w Kościerzynie. 2020 rok może być okresem spektakularnych działań w cyberprzestrzeni organizacji przestępczych wspieranych przez mocodawców instytucjonalnych. Tego typu grupy cyberprzestępców rozlicza się z np. udanego blokowania działania danej infrastruktury. Ale mocodawcy często przymykają nieco oko na to, co cyberprzestępcom da się zdobyć dla siebie „przy okazji”. To może oznaczać wzrost liczby ataków na użytkowników prywatnych.

Sławomir Pijanowski - iGRC Executive Consultant Atos

Cyberbezpieczeństwo w sektorze obronnym to temat priorytetowy. Na sektor obronności przenoszą się napięcia i konflikty polityczne w różnych miejscach świata i w związku z tym tzw. dominacja informacyjna jest dzisiaj kluczem do sukcesu. W takiej rzeczywistości decyzje w obszarze obronności 2020+ powinny uwzględnić następujące aspekty: kooperatywna walka żołnierz wspomagany rzeczywistością rozszerzoną, taktyczne komunikowanie się, zarządzanie danymi i cyberbezpieczeństwo. Dane i informacje należy traktować jako broń, dlatego procesy zarządzania danymi z wykorzystaniem technologii IoT, sztucznej inteligencji, uczenia maszynowego, technologii roju i szyfrowania kwantowego są tak ważne. Dzięki posiadanym danym stanie się możliwa analiza predykcyjna w czasie rzeczywistym - możliwości przewidywania zachowań wroga na podstawie otrzymanych danych. Dlatego zdolność do ochrony tych danych stanowi o przewadze w walce i pozwala na bieżąco korygować strategie ataku jak i obrony.

Zespół CyberRescue (mAccelerator)

W nadchodzącym roku głębokie nadzieje pokładam w chmurze. To tam będzie przenosił się biznes i wszystkie jego części składowe. Myślę, że inwestowanie w automatyzację obszaru cyberbezpieczeństwa w firmach będzie stanowiło też istotny element w udaremnianiu prób włamań, które mają miejsce w biznesie. Głęboko wierzę, że wprowadzenie Dyrektywy PSD2 wzmocni jeszcze bardziej bankowość online. Jednak do najbardziej dominujących trendów należy zaliczyć rozwój maszynowego uczenia się i szeroko pojętej sztucznej inteligencji. Warto skupić uwagę na inwestowanie w struktury bezpieczeństwa sektorów publicznych. W szczególności infrastruktury krytycznej, jak szpitale czy elektrownie.

Jarosław Mastalerz - partner zarządzający mAccelarator

2020 to z pewnością rok głębokiego rozwoju sztucznej inteligencji. To na AI i maszynowe uczenie zarządy firm powinny położyć największy nacisk. Stanowi to najbardziej efektywne rozwiązanie mające na celu zwiększenie bezpieczeństwa. Właśnie to rozwiązanie daje możliwość weryfikacji nowych zagrożeń. W 2020 roku największe firmy, instytucje państwowe, a nawet mniejsze przedsiębiorstwa będą starały się zainwestować we wdrożenie rozwiązań sztucznej inteligencji. Mam głęboką nadzieję, że użytkownik Internetu w 2020 to człowiek bardziej świadomy zagrożeń, dbający o swoją prywatność w Internecie.