Cyberdefence 24

11.01.2019

PROGNOZY CYBERBEZPIECZEŃSTWA NA ROK 2019

Straty spowodowane cyberatakami przekraczające bilion dolarów, amerykańskie RODO, dalsza militaryzacja cyberprzestrzeni oraz test realnego wdrażania Ustawy o KSC to prognozy ekspertów na rok 2019 w obszarze cyberbezpieczeństwa.

Artur Marek Maciąg – Inicjatywa Kultury Bezpieczeństwa

Bezpieczeństwo ludzi i zasobów w sieci zależy od tak wielu czynników, że określanie jego trendów jest jak prognozowanie pogody. Głównym czynnikiem zmian krajobrazu będą eksperymenty z użyciem uczenia maszynowego i sztucznej inteligencji oraz robotyzacji procesów zarówno dla zapewnienia bezpieczeństwa jak i przełamania zabezpieczeń. Przestrzeń urządzeń, systemów, aplikacji i danych obecna będzie przedmiotem nowych prób regulacji prawnych, w tym ściślej skonkretyzowanych na etyczne postępowanie zarówno algorytmów jak i ludzi.

Rynek usług cyfrowych przywita usługi certyfikacji na potrzeby RODO/GDPR i cyberbezpieczeństwa, które wspomogą i wzbogacą istniejące oferty ubezpieczeń od cyberryzyk. W zakresie zagrożeń globalnych, człowiek jako „czynnik ludzki" będzie uwikłany w jeszcze większy odsetek incydentów, między innymi z uwagi na zastosowanie języka naturalnego w mechanizmach spamu i phishingu oraz postępujące zmęczenie na skutek przeciążenia nieistotnymi informacjami. Sieci społeczne przemodelują swoje oferty pogłębiając problem pozornej kontroli nad danymi i prywatnością użytkowników. Rynek handlu podatnościami i bronią cybernetyczną doczeka się formalizacji i regulacji.

Obecna wojna w cyberprzestrzeni doprowadzi do kilku gorących incydentów, odwracając uwagę od bieżących problemów politycznych lub gospodarczych wewnątrz państw, których cyber wojska będą zaangażowane w te konflikty. Coraz więcej państw będzie zgłaszało gotowość lub ambicje do przystąpienia do światowej wojny w cyberprzestrzeni pod pretekstem obrony i ochrony wewnętrznej infrastruktury krytycznej. W zakresie gospodarstwa domowego i ekonomii cyfrowej spodziewać się można rozwoju technologii ubieralnej oraz protokołów wymiany danych opartych na blokchainie, w tym i popularyzacji płatności. Bez wątpienia rok 2019 będzie rokiem w którym zaufanie zostanie zastąpione kontrolą, cyfryzacja realnie zajrzy pod strzechy każdego gospodarstwa domowego a komputer kwantowy zademonstruje swoją moc w zakresie kryptografii. Nie zmieni się zapewne problem używania haseł dostępu do zasobów, bezpieczeństwa urządzeń mobilnych i oszustw dla płatności za usługi w Internecie.

Izabela Albrycht – Prezes Instytutu Kościuszki

Postępująca aplikacja coraz to nowszych technologii informatycznych do wszystkich sektorów gospodarki, a także przenikanie się tych technologii oraz automatyzacja ataków hackerskich (dzięki zastosowaniu sztucznej inteligencji i uczenia maszynowego) sprawi, że wzrośnie liczba ataków, a także stopień ich zaawansowania, co wymagać będzie odpowiedniego dostosowania działań defensywnych ze strony użytkowników sieci i systemów IT. Bezpieczeństwo sieci komórkowej 5G w

ujęciu całego cyfrowego łańcucha wartości będzie jednym z najważniejszych tematów pierwszej połowy roku i będzie przedmiotem dyskusji i regulacji ze strony rządów i organizacji międzynarodowych takich jak UE.

Joanna Świątkowska – Dyrektor Programowy Europejskiego Forum Cyberbezpieczeństwa (CYBERSEC)

Rok 2019 upłynie pod znakiem zmagań dyplomatycznych dotyczących międzynarodowych aspektów cyberbezpieczeństwa. Będziemy obserwowali dalsze zderzenie dwóch wizji tego jak powinny kształtować się działania prowadzone w cyberprzestrzeni. Jedna reprezentowana jest przez „blok zachodni", druga przez „blok wschodni" z Rosją i Chinami na czele. Sygnałem zapowiadającym napiętą sytuację były wydarzenia na forum ONZ, w tym przyjęcie dwóch rezolucji dotyczących dalszych prac na rzecz bezpieczeństwa w cyberprzestrzeni. Dodatkowo obserwować będziemy wzmożone działania na gruncie atrybucji i znalezienia właściwej odpowiedzi na cyberataki. Szczególnie aktywna będzie tutaj UE, która będzie szukała konsensusu w zakresie stosowania Cyber Diplomacy Toolbox, nie zabraknie także solidarnych działań „koalicji" podobnie myślących państw. Uważam, że jeszcze mocniej widoczne będą działania podmiotów prywatnych, szczególnie firm technologicznych, które będą chciały aktywnie wpływać na rozwój wydarzeń w tym obszarze.

W 2019 nastąpi ugruntowanie funkcjonowania istniejących kluczowych regulacji i dalsza ich, szczegółowa implementacja. W 2019 roku będziemy obserwowali praktyczne działania na rzecz dalszego wdrażania Dyrektywy NIS zarówno w wymiarze państw jak i w obszarze międzynarodowym. Kluczowe będzie także wzmocnienie działania ENISY oraz rozwój działań związanych z certyfikacją. Interesujące będzie także to jak rozwinie się wpływ RODO na podejście innych (pozaeuropejskich) graczy w zakresie tworzenia ich regulacji związanych z ochroną prywatności.

Ireneusz Piecuch – Partner w Kancelarii Gawroński & Piecuch

Rok 2019 przywitał nas kolejną mega-cyber-wpadką. Tym razem ponad 380 milionów rekordów klientów sieci Marriot dołączyło do światowych megazasobów wykradzionych informacji. W Stanach Zjednoczonych rozpętało to dyskusję na temat gromadzenia i przetwarzania danych bez precyzyjnych reguł dotyczących dopuszczalnego zakresu oraz okresu ich przechowywania, podczas gdy europejscy wyznawcy spod znaku regulacji 4.0 po raz kolejny potraktowali to jako świadectwo wyższości europejskiego podejścia do wyzwań rewolucji cyfrowej. I to właśnie regulacje będą tematem przewodnim w nadchodzących 12 miesiącach. Stany Zjednoczone dopracują się swojego RODO, my zapoznamy się z praktycznym aspektem regulacji wprowadzonej w połowie 2018 – czyli z karami nakładanymi przez regulatora. Krajowy System Cyberbezpieczeństwa obudowany zostanie aktami wykonawczymi, zaleceniami, opiniami, instrukcjami, które sprawią, że wszyscy będą mieć pełne ręce roboty więc na wprowadzenie realnych zmian mających spowodować wzrost świadomości oraz wzrost odporności na cyberzagrożenia najzwyczajniej zabraknie czasu. W tym wszystkim świetnie odnajdą się organizacje czerpiące krocie z ataków na systemy teleinformatyczne. Podobnie jak to było w latach poprzednich ich wydatki na nowoczesną technologię przekroczą wydatki ponoszone na zabezpieczenie systemów od ośmiu do dziesięciu razy. I będzie to inwestycja ze wszech miar uzasadniona gdyż, szacowane na 600 miliardów dolarów straty wyrządzone przez różnego rodzaju ataki na systemy teleinformatyczne w roku 2017 mogą już w tym roku zbliżyć się do jednego biliona dolarów. Czy nam się to podoba czy nie, świat staje się coraz bardziej cyfrowy, coraz bardziej mobilny, coraz bardziej uzależniony od cyfrowej identyfikacji. Może zatem hasłem przewodnim na ten rok powinno być, wzorem kampani prezydenckiej Billa Clintona, zawołanie „Cyberbezpieczeństwo głupcze !" ?

Zdzisław Wiater – Dyrektor Obszaru Cyberbezpieczeństwa, Asseco Poland

W 2019 głównym tematem będzie konkurencja pomiędzy USA i Chinami oraz związane z nią oskarżanie Chin o wykorzystywanie dostarczanego klientom sprzętu w celu nielegalnego zbierania danych. Podłoże tego konfliktu jest co prawda głównie handlowe i wiąże się z próbą powstrzymania ekspansji producentów z Chin, jednak będzie to problem, z którym odbiorcy technologii będą musieli sobie w przyszłym roku poradzić. Odpowiedzią na ten problem mogą być programy certyfikacji i badań produktów na spełnianie wymogów cyberodporności, izolowanie sprzętu zewnętrznych producentów (bez znaczenia czy pochodzących z Chin czy od innego dostawcy) za pomocą narodowych rozwiązań lub tworzenie kluczowych elementów sprzętowych we własnym zakresie i tam, gdzie jest to możliwe. Na rynku krajowym duże zmiany przynieść może wejście w życie ustawy o Krajowym Systemie Cyberbezpieczeństwa. Wiązać się to może ze zwiększeniem dynamiki rozwoju rynku usług SOC a także, w dłuższej perspektywie, doprowadzić do pojawienia się innowacyjnych produktów z obszaru cyber.

Marcin Spychała – **Senior Security Architect IBM**

Większość specjalistów od cyberbezpieczeństwa nie lubi pytań o przyszłość cyberzagrożeń. Nie dlatego że są to pytania trudne, a dlatego że są to pytania które otrzymują najczęściej – niejednokrotnie z prośbą o zawarcie odpowiedzi jedynie w kilku zdaniach. W takim przypadku najlepszą odpowiedzią wydaje się być że powinniśmy się spodziewać tego co dotychczas tylko w większej skali. Więcej złośliwego oprogramowania, więcej przejmowania kont i więcej nakierowanych ataków phishingowych. Ilość wyciekających danych również rośnie rok do roku i nie widać powodów, dla których 2019 miałby być rokiem pod tym względem wyjątkowym. Jednocześnie większość zjawisk nowych lub nietypowych będzie niezauważalna dla przeciętnego obywatela z racji ich niszowości lub poziomu skomplikowania.

Niemniej jednak można przypuszczać, że rok 2019 będzie wyjątkowy i unikatowy pod paroma względami. Przede wszystkim w ramach Unii Europejskiej będziemy mieli cały czas do czynienia z niespodziewanymi skutkami wprowadzenia regulacji RODO. Do tej kategorii należy niewątpliwie zaliczyć niemożliwość korzystania z bazy WHOIS przy identyfikacji złośliwych domen i aktorów za nimi stojących, gdyż zgodnie z RODO dane te muszą pozostać zamaskowane. Tego typu niespodziewane konsekwencje regulacji spotykamy na każdym kroku, ale nie każde ma tak fundamentalne skutki dla walki ze złośliwymi domenami. Rok 2019 powinien przynieść, jeśli nie zmianę regulacji to przynajmniej zmianę wykładni stosowanych przepisów żeby przy okazji idei ochrony danych osobowych nie wylać dziecka z kąpielą.

Kolejnym zjawiskiem, które może być odczuwalne w 2019 jest wzrost rachunków na prąd w związku z nielegalnym wykorzystywaniem infrastruktury przedsiębiorstwa do kopania kryptowalut. Same zjawisko nie powoduje wprawdzie utraty danych czy uszkodzeń w infrastrukturze – ale przykład Coinhive pokazuje jak szybko rynek adaptuje takie technologie do działań niezgodnych z ich przeznaczeniem.

Niezależnie od poszczególnych ataków czy zagrożeń punktowych, dużym trendem w obszarze zagrożeń jest coraz bardziej wektor zagrożeń mobilnych. I nakładają się na to dwa niezależne trendy. Pierwszym jest niewątpliwie wzrost stopnia zaawansowania złośliwego oprogramowania przeznaczonego na urządzenia mobilne (na przykład malware Android.Banker.L typu „all-in-one”) oraz nakładający się na to trend wychodzenia z dystrybucją poza oficjalne sklepy producentów systemów operacyjnych Google Play i AppStore. Sama motywacja producentów aplikacji jest tutaj oczywista, ale z perspektywy bezpieczeństwa można się spodziewać znaczącego wzrostu infekcji urządzeń mobilnych.

Ostatnim trendem który w 2019 nadal będzie rosnącym będzie zwiększona aktywność botów mediów społecznościowych. I jakkolwiek nie jest to może bezpośrednie zagrożenie infrastruktury

przedsiębiorstwa ale jest niewątpliwie krytyczne w skali całych gospodarek zarówno z perspektywy kształtowania podaży i popytu jak również kształtowania postaw w skali całych społeczeństw.

Mirosław Maj – Prezes Fundacji Bezpieczna Cyberprzestrzeń

Uważam, że w 2019 roku dojdzie do jeszcze większego zaognienia sytuacji dotyczącej wykorzystania cyberataków w konfliktach politycznych. Na tym polu kilka państw, przede wszystkim, USA, Chiny, Rosja, Iran i Izrael, chce systematycznie zaznaczać swoją obecność. Kwestia ustalania atrybucji jest w praktyce przegrana. Nie tylko od strony technicznej, ale również z tego powodu, że nikt się tymi wskazaniami nie przejmuje. Co więcej - mam wrażenie, że niektórzy z przyjemnością odnotowują wskazywanie ich palcem. Sytuacje mogłoby jedynie zmienić międzynarodowe prawo dotyczące poważnych konsekwencji za takie akty, ale na takowe się nie zanosi. Do grona ważnych graczy w tym obszarze zgłosi akces kilku nowych graczy - Turcja, Indie, może Nigeria. Moim marzeniem jest, żeby wśród nich była Polska, ale niestety nie podaję tego w swoich przewidywaniach.

Myślę też, że w nadchodzącym okresie może wzrosnąć w Europie presja regulacyjna wobec największych graczy takich jak Google czy Facebook. Ich potęga rośnie do takich rozmiarów, że władze wielu państw zaczną się jej obawiać. Regulacja, kary, ograniczenia pozostaną dla polityków nich jedynym orężem. Pretekstem może być zamieszanie towarzyszące wyborom do parlamentu europejskiego.

W krajowym podwórku, nie tyle przewiduję, co wyrażam nadzieję, że 2019 będzie pozytywnym testem realnego wdrażania Ustawy o KSC. Uznałbym, że tak się stało jeśli podjęte by zostały pierwsze decyzje o sektorowych CERT-ach, zorganizowano by krajowe ćwiczenia, zainicjowane przez Pełnomocnika i w planie budżetu na 2020 pojawiłby się sensowny budżet na wdrożenie KSC. Dodatkowo przewiduję burzliwą dyskusję wokół technologii 5G, i to że kwestie cyberbezpieczeństwa będą ją w dużym stopniu kształtowały. Raczej nie z punktu widzenia technologicznego, a strategiczno-politycznego.