aut. Andrzej Kozłowski 28.12.2017

PROGNOZY CYBERBEZPIECZEŃSTWA NA ROK 2018 [ANALIZA]

Redakcja CyberDefence24.pl zapytała eskpertów ds. cyberbezpieczeństwa z Polski i świata o trendy cyberbezpieczeństwa na rok 2018. Odpowiedzieli udzielili Jakub Syta, Dyrektor Biura Bezpieczeństwa EXATEL S.A., Joanna Świątkowska Dyrektor Programowy Europejskiego Forum Cyberbezpieczeństwa CYBERSEC, Generał Włodzimierz Nowak – Członek Zarządu T-Mobile Polska, Dyrektor ds. Prawnych, Bezpieczeństwa i Zarządzania Zgodnością, dr Łukasz Olejnik, konsultant i badacz cyberbezpieczeństwa, Michał Jarski z Wheel Systems, Maciej Ostasz z Fundacji Centrum Analiz Propagandy i Dezinformacji oraz Philip Chertoff z GLOBSEC Policy Institute

JAKUB SYTA – Dyrektor Biura Bezpieczeństwa EXATEL S.A.

Mijający rok był wyjątkowo udany dla cyberprzestępców. Obserwowaliśmy ogólnoświatowe infekcje, skuteczne ataki na dostawców oprogramowania, masowe stosowanie wodopojów, gigantyczne wycieki danych i kradzieże e-walut. Tego typu działań z pewnością nie zabraknie w przyszłym roku.

Spodziewam się, że w 2018 roku gwałtownie wzrośnie też liczba ataków, których celem będzie kradzież danych i szantaż ich ujawnieniem. Po 25 maja 2018 roku organizacje, które je stracą mogą zostać obciążone potężnymi karami. A do wejścia w życie tych przepisów przygotowują się nie tylko pracownicy IT i prawnicy, ale i cyberprzestępcy licząc na okup płacony przez szantażowane firmy.

Drugim trendem mogą być ataki bazujące na zaufaniu do producentów oprogramowania (tzw. supply chain attacks). Przestępcy przełamują zabezpieczenia i podkładają fałszywą wersję programu. Skutki tego typu ataku nie raz doprowadzą do paraliżu setek, jeżeli nie tysięcy organizacji.

W maju wchodzą też w życie dyrektywy GDPR oraz NIS, które również będą kształtowały rynek cyberbezpieczeństwa. Ich zapisy mówią o konieczności monitorowania i reagowania na incydenty przez wszystkich uczestników wirtualnego świata. To spowoduje, że przedsiębiorcy wreszcie zaczną poważnie podchodzić do kwestii logowania zdarzeń i ich stałego monitorowania tak, by móc samodzielnie wykryć atak. Tym samym przyszły rok powinien stać się rokiem rozkwitu usług typu Security Operations Center (SOC).

Przede wszystkim mam jednak nadzieję, że 2017 rok zakończy okres udawania, że „u nas jest dobrze" i „nas to na pewno nie dotknie". Każdy jest potencjalnym celem. Atrakcyjność i zyski z cyberataków są zbyt duże, by je bagatelizować. A kary będą ogromne.

Czytaj więcej: 2017 rokiem ofensywy Rosji i Chin w cyberprzestrzeni?

Joanna Świątkowska – Dyrektor Programowy Europejskiego Forum Cyberbezpieczeństwa CYBERSEC

Przyszły rok upłynie z pewnością pod znakiem ważnych debat związanych z cyberbezpieczeństwem Unii Europejskiej. Spodziewam się, że wiele tematów zaproponowanych w tak zwanym pakiecie cyberbezpieczeństwa będzie w centrum uwagi. Jednym z nich z pewnością będzie kwestia certyfikacji.

Rok 2018 będzie także mocno naznaczony implementacją Dyrektywy NIS oraz początkiem obowiązywania RODO. Oba procesy bardzo mocno zmienią krajobraz cyberbezpieczeństwa w Europie.

Z punktu widzenia megatrendów – najbliższe miesiące i lata to z pewnością wyzwania jakie niosą nowe technologie, szczególnie sztuczna inteligencja i blockchain. Oczywiście w ślad za nimi pójdzie wiele korzyści, ale także wiele znaków zapytania. Na przykład w jaki sposób AI może być użyte do prowadzenia walki informacyjnej i jak temu zapobiegać.

Z punktu widzenia krajowej polityki – oczywiście kluczowy będzie ostateczny kształt ustawy o cyberbezpieczeństwie oraz Planu Działań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022. Zasadniczą role odegraj kroki związane z ich implementacją.

Czytaj więcej: Ekspert: Francja i Niemcy na celowniku hakerów w 2017 roku

Generał Włodzimierz Nowak – Członek Zarządu T-Mobile Polska, Dyrektor ds. Prawnych, Bezpieczeństwa i Zarządzania Zgodnością

Celem ataków przestępców są już nie tylko nasze komputery, laptopy czy telefony, a coraz częściej routery i sieci WiFi. Tak jak dotychczas w 2018 roku dominować będą przestępstwa polegające na: wyłudzeniach, m.in., poprzez usługi premium lub fałszywe faktury, kradzieży środków z konta bankowego użytkownika, czy szantażu pod groźbą fizycznego zniszczenia sprzętu oraz usunięciu lub upublicznieniu danych.

Fot. Public Domain Pictures/Domena Publiczna

Wraz ze wzrostem popularności rozwiązań typu smart możemy się spodziewać, że również tam przestępcy mogą szukać okazji do zarobku np. przejmując kontrolę nad urządzeniami. Pomimo tego, że charakter ataków pozostanie podobny można się spodziewać, że z roku na rok będzie ich coraz więcej. Postęp technologiczny otwiera też pole do nowego obszaru ataków cybernetycznych na niezabezpieczoną infrastrukturę IoT. Obrona tej infrastruktury będzie poważnym wyzwaniem dla ekspertów cyberbezpieczeństwa.

Czytaj więcej: Bezpieczeństwo WiFi to mit. Każde urządzenie zagrożone

Dr Łukasz Olejnik, konsultant i badacz cyberbezpieczeństwa i prywatności, afiliowany przy Center for Information Technology Policy Uniwersytetu Princeton. Autor Prywatnik.pl

Z pewnością rok 2018 będzie kolejnym rokiem prywatności; wręcz momentem przejścia. I nie chodzi jedynie o nadużycia i dużej skali wycieki danych. To swoją drogą, ale będzie też pozytywnie! Stanie się tak dzięki General Data Protection Regulation, w Polsce w skrócie zwanej RODO.

RODO to znacznie lepsze niż obecnie rozwiązania dla użytkowników, obywateli, konsumentów. Zwiększają one ochronę prywatności, dają więcej kontroli. W wielu przypadkach RODO będzie także po prostu dużą motywacją do podniesienia poziomu nie tylko prywatności, ale i cyberbezpieczeństwa – większą niż te wynikające z Dyrektywy NIS

To prawda, że RODO to duże wyzwanie dla firm i organizacji, zwłaszcza niektóre z jego wymogów takich jak Privacy by Design czy analiza poziomu ochrony prywatności i danych przy okazji konieczności oceny skutków dla ochrony danych (DPIA). Ostatecznie okaże się więc, że wiele firm nie

będzie gotowych na czas – włączając to też i te uważające przeciwnie. RODO będzie wyzwaniem dla instytucji publicznych, rządowych, a nawet tych odpowiedzialnych za ochronę danych. Czy w 2018 w Europie zostanie nałożona na jakiś podmiot maksymalna kara RODO liczona w milionach euro? Jeśli tak, to nie powinno być to zaskakujące.

Czytaj więcej: RODO wyzwaniem dla polskich firm (SecureTech Congress)

Michał Jarski – wiceprezes i dyrektor zarządzający w Wheel Systems w regionie Europy, Bliskiego Wschodu, Afryki i Azji

Przypuszczam, że przyszły rok w cyberbezpieczeństwie upłynie nam pod znakiem człowieka. Począwszy od naszych danych osobowych, na których straży ma stać RODO/GDPR. W maju 2018 będziemy świadkami kilku spektakularnych katastrof: ogromnych wycieków danych jakie wyjdą na jaw (również przy aktywnym udziale konkurujących firm uprzejmie donoszących do regulatora), pierwszych kar idących w miliony euro, ale także zatkania systemu kontroli napływem zgłoszeń naruszeń, próśb o certyfikację etc.

Również pod kątem człowieka, jako najsłabszego ogniwa zarówno po stronie użytkowników systemów (bo to oni na koniec dnia ulegają manipulacjom i uruchamiają załączniki w mailach albo zwyczajnie kradną dane), ale także zarządzających bezpieczeństwem systemów IT, bo zwyczajnie przestaną sobie radzić z narastającą falą podatności. Już teraz widać, że człowieka musi zacząć wspomagać sztuczna inteligencja zastępując tradycyjne metody identyfikacji i neutralizacji zagrożeń. Będą to oparte o machine learning mechanizmy wyłapywania anomalii zachowań użytkowników, ruchu sieciowego oraz korelujące informacje z wielu źródeł i reagujące bez ingerencji człowieka. To niestety odnosi się także do systemów kontrolujących zachowania społeczne, jak to już widzimy w Chinach (Social Credit System i powszechna inwigilacja).

Czytaj więcej: Internet rzeczy czy internet zagrożeń? [ANALIZA]

Idąc tą drogą, przewiduję, że ludzie coraz bardziej uzależnieni od wszechogarniającej nas automatyzacji i „internetu rzeczy" doświadczą w nadchodzącym roku boleśnie skutków przejęcia kontroli nad ich życiem. A może nawet rzeczywistej katastrofy na większą skalę spowodowanej „buntem maszyn" – błędem w funkcjonowaniu algorytmów sterujących na przykład ruchem pociągów, samochodów lub innej powszechnej usługi. Przy czym może to być także połączenie błędu konstrukcyjnego z aktywnym włamaniem i modyfikacją systemu przez ludzi o złych zamiarach.

Internet of things / pixabay.com

Maciej Ostasz, ekspert IT Fundacji Centrum Analiz Propagandy i Dezinformacji

Rok 2017 pokazał jak silnym zagrożeniem są ransomware'y. Choć producenci sprzętu i oprogramowania wzięli mocno do siebie ataki i zaczęli zapobiegać tego typu zagrożeniom, WannaCry jak i Petya odsłoniły niedoskonałości cyfrowego świata. W nowym roku możemy zobaczyć mutacje, nie tyle ransomware'ów, co exploitów opartych o mechanizmy narzędzia EternalBlue.

Czytaj więcej: „Petya/NotPetya – analiza tajemniczego malware'u który zaatakował Ukrainę" (SCS 2017)

Patrząc na zaangażowanie producentów, nowe zagrożenia na pewno będą wymierzone bezpośrednio w użytkowników, a to oznacza rozwój socjotechnik oraz sposobów dystrybucji złośliwego oprogramowania w na poziomie internetu, intranetu jak i sieci globalnej. Największą niewiadomą jest to, w jaki sposób można jeszcze wykorzystać wykradzione narzędzia NSA oraz jak szerokie spektrum działania może mieć takie oprogramowanie oraz jakie konsekwencje po 25 maja będą ponosić firmy i instytucje w przypadku wycieku danych za pomocną nieznanych luk bezpieczeństwa.

Siedziba NSA w Fort Meade, Maryland. Fot. wikipedia.org

Philip Chertoff - GLOBSEC Policy Institute

Pod koniec tego roku kilka państw ogłosiło stworzenie własnych dowództw ds. operacji w cyberprzestrzeni, które mają pomoc w rozwoju ofensywnych jak i obronnych zdolności w środowisku wirtualnym.

W 2018 roku możemy oczekiwać, że więcej państw zdecyduje się na podobny krok oraz, że cześć tworzonych dowództw osiągnie poziom gotowości operacyjnej. Pomimo planów ze strony NATO i UE, państwa skupią swój wysiłek oraz inwestycje na rozwoju narodowych zdolności w cyberprzestrzeni.

Czytaj więcej: UE: nowe struktury cyberbezpieczeństwa i unijne centrum badawcze

Pomimo tego, że istnieje niewielkie prawdopodobieństwo, że NATO i UE zrobią zdecydowany postępu w operacjonalizacji własnych zdolności w cyberprzestrzeni, ich współpraca powinna jednak wpłynąć pozytywnie na stworzenie wspólnego języka opisującego operacje w cyberprzestrzeni. Ponadto obie organizację mogą stworzyć zbiór wytycznych odpowiedzi na cyberataki ataki oraz sformułować niezbędne zdolności w tzw. skrzynce odpowiedzi Unii Europejskiej na cyberataki.

Fot. wikipedia.org

Podczas gdy rządy i korporacje skupiły się głównie na zagrożeniach dla dostępności i poufności danych, ostatnie działania dezinformacyjne spowodowały, że obserwujemy powrót na agendę kwestii związanych z integralnością danych.

Możemy oczekiwać wzrastających liczby dyskusji o ryzku możliwości manipulacji danymi i potrzebie zapewnienia ich integralności w wielu sektorach cywilnych (sektor finansowych, opieka zdrowotna, awiacja).