WANNACRY I PETYA/NOT PETYA. LEKCJA NA PRZYSZŁOŚĆ: POTRZEBUJEMY CYBERNETYCZNEGO CENTRUM EPIDEMIOLOGII [ANALIZA]

Ostatnie skoordynowane ataki ransomware (albo cyberepidemii, jak lepiej je nazywać) uświadomiły nas o prawdopodobnym istnieniu nowego, globalnego zagrożenia. Abstrahując od istoty ataku (ransomware, malware, broń cybernetyczna), jego wektora oraz sprawcy (grupa przestępcza, służby państwowe czy haktywiści), musimy zmienić swoje podejście do globalnych zagrożeń cybernetycznych. Żyjemy w świecie połączonym urządzeniami IP, a nasza sieć komputerowa nie jest niezależna. Przestrzeń i odległość przestały mieć znaczenie i po prostu nie jesteśmy w stanie odizolować geograficznie pewnych zagrożeń, tak jak dawniej medycyna nie była w stanie odizolować epidemii. Proponowanym rozwiązaniem byłby model prewencji i odpowiedzi na globalne zagrożenia cybernetyczne oparty na doświadczeniach Światowej Organizacji Zdrowia.

Jak wygląda dziś międzynarodowa współpraca w zakresie cyberbezpieczeństwa?

Obecną współpracę międzynarodową porównać można do okresu przed założeniem Światowej Organizacji Zdrowia. Do czasu wybuchu II wojny światowej państwa nie miały oficjalnej platformy dla wypracowania wspólnych rozwiązań dla zagrożeń zdrowotnych takich jak cholera, tyfus, febra. Podobnie w XXI wieku, rządom brakuje międzynarodowej organizacji dla przeciwdziałania cyberepidemiom.

Czytaj też: Petya - WannaCrya na sterydach. Kolejny globalny atak ransomware.

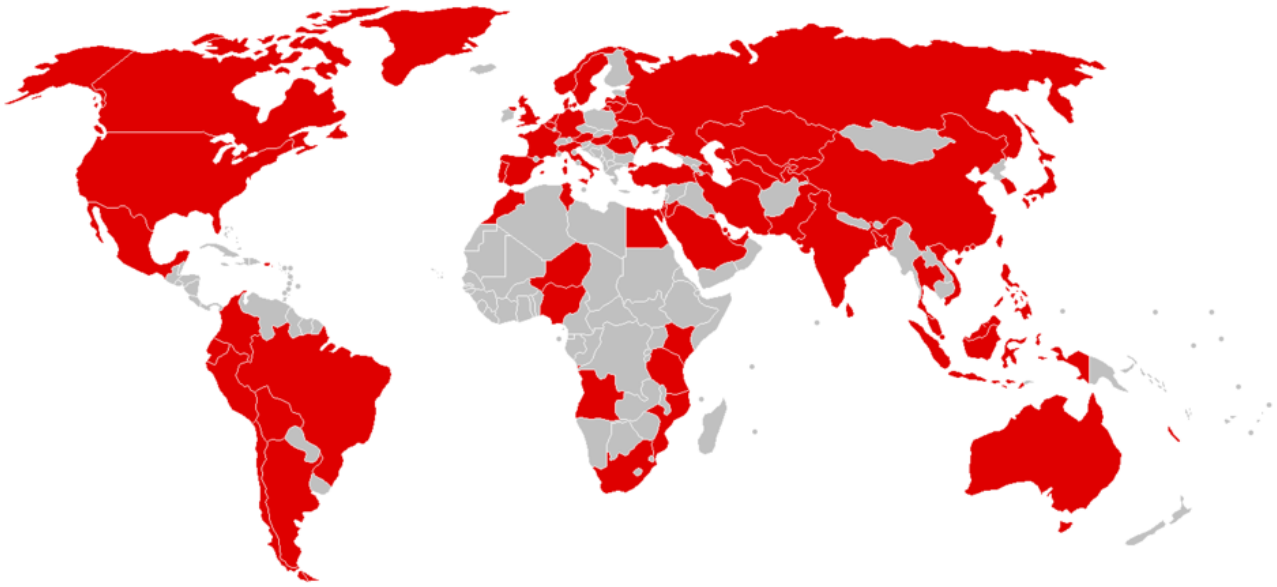
Prawie każdy z rządów posiada niezależny CERT - Computer Emergency Response Team i CIRT – Computer Incident Response Team. Sojusze wojskowe, jak NATO, posiadają własne centra reagowania i centra kształcenia w rodzaju Cooperative Cyber Defence Centre of Excellence w Tallinie. Światowe firmy IT i sektor finansowy inwestują we własne ośrodki. Organizacje takie jak UE tworzą wyspecjalizowane agencje ENISA. Tuzin innych niezależnych firm z obszaru informatyki śledczej, NGOs, instytuty, akademie zajmują się kwestiami cyberbezpieczeństwa. Międzynarodowe organizacje wspierające pracę policji, takie jak Interpol i Europol, zbierają dane o cyberprzestępstwach.

Czytaj też: Szyfrowanie danych sposobem na ransomware [Cyberdefence24.pl TV].

ONZ jednak nie uczestniczy w globalnej odpowiedzialności za zagrożenia cybernetyczne. Międzynarodowy Związek Telekomunikacyjny (ITU) jest obecnie jedyną organizacją podlegająca ONZ, która aktywnie akcentuje globalne problemy przestrzeni wirtualnej. Jednakże ITU ma funkcję bardziej doradczą niż operacyjną. Ponadto organizacja nie przyciąga decydentów i nie zabezpiecza im jednej platformy do spotkań.

ITU porusza problematykę cyber bezpieczeństwa na dwóch płaszczyznach:

1. W formie statycznej i analizie porównawczej – Global Cybersecurity Index (pierwsze edycja 2014 i najnowsza w 2017 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf). Przypomina to trochę generowane od kilku dekad indeksy zdrowia i statystyki medyczne publikowane przez Światową Organizację Zdrowia. W każdym razie statystyka i analiza porównawcza pomaga zobaczyć całość obrazu.
2. W formie propagowania cyberhigieny. Podobnie jak ma to miejsce w teorii medycyny, wirus atakuje najsłabszy organizm, po czym rozprzestrzenia się, duplikuje się, mutuje i atakuje kolejne organizmy. Podatne są na niego organizmy o najniższym poziomie higieny.



Fot. Roke / Wikipedia / CC 3.0 domena publiczna

Jakie rozwiązania przyjąć?

Powinniśmy stworzyć model cyberepidemiologii oparty na doświadczeniach Światowej Organizacji Zdrowia.

ONZ nie może polegać na roli ITU w zwalczaniu zagrożeń w cyberprzestrzeni, ponieważ nie została ona założona w tym celu. Powinna powstać nowa organizacja wyspecjalizowana, na przykład WCSO – World Cyber Security Organization. Decydenci (rządy państw i biznes) muszą spotkać się wirtualnie na jednej platformie, aby omówić najbardziej palące problemy.

Czytaj też: CERT Polska - atak Petya & Mischa.

Powinniśmy stworzyć centra cyberepidemiologii w celu testowania nowych rozwiązań, cybernetycznych „szczepionek" i modeli reagowania. Medyczna teoria „pacjenta zero" byłaby w pełni relewantna dla analizy kodu, załatania podatności w najkrótszym możliwym czasie. Potrzeba stworzenia takiego centrum kryzysowego jest tym bardziej aktualna w dobie dominacji internetu rzeczy.

Aktualne ataki ransoware czy malware są swoistym nawiązaniem do medycznych teorii spiskowych. Zgodnie z nimi wielkie koncerny farmaceutyczne często obwiniane są o produkcję jakiegoś wirusa, a potem odkrycie szczepionki i zarobienie - dzięki temu - ogromnych pieniędzy. Podobnie autorzy ransomware, najpierw tworzą malware i jedynie oni posiadają klucz odszyfrowujący. W przypadku globalnej cyberkatastrofy klucz odszyfrowujący byłby nie mniej cenny niż szczepionka w przypadku pandemii. Musimy sobie uświadomić, że jako ludzie nie chcemy być zakładnikami własnych

technologii.

Jest kwestią czasu kiedy pojawi się nowa mutacja malware. Ponieważ społeczeństwo coraz bardziej zdaje się na rozwiązania technologiczne, wyobraźmy sobie katastrofę, do jakiej może dojść w momencie udanego ataku na globalne systemy płatnicze: SWIFT lub Blockchain. Człowiek funkcjonuje w dwóch paralelnych rzeczywistościach: fizycznej i wirtualnej. Wcześniej czy później granica między tymi rzeczywistościami stanie się niezauważalna. Szczególnie wtedy, kiedy zagrożenia cybernetyczne będą miały efekt kinetyczny: preludium był Stuxnet i Blackenergy.

Paweł Góralski

#PAS17 PARYSKI DEBIUT F-35 I INNE LOTNICZE PREMIERY [GALERIA] | @Defence24pl