TRANSKRYPCJA – Odcinek XXI

Konflikt nie tylko militarny. Cyberaspekty wojny v2

[00:00:07]

Prowadzący: Cześć. Witam wszystkich słuchaczy w kolejnym odcinku naszego podcastu. Obecna sytuacja za naszą wschodnią granicą nie napawa optymizmem. Scenariusze, których jesteśmy świadkami powodują z jednej strony racjonalną obawę o bezpieczeństwo granic, zdrowie i życie ludzkie, z drugiej – masę domysłów, spekulacji czy dezinformacji. Wojna, z którą mamy do czynienia nie jest tylko konfliktem zbrojnym i chyba wszyscy sobie z tego faktu zdajemy sprawę. Jest to wojna, w której ważnym aspektem są również działania dezinformacyjne, destabilizacja stron, również z wykorzystaniem aspektów cyber, które mogą być bardzo niebezpieczne. Z jakimi możliwościami mamy do czynienia biorąc pod uwagę wszystkie strony? Jak wygląda cyberaspekt wojny? Czego tak naprawdę jesteśmy świadkami? I co jeszcze może nas czekać w najbliższym czasie? O tym już za chwilę. „Konflikt nie tylko militarny. Cyberaspekty wojny". Moim dzisiejszym gościem jest Mirosław Maj, wieloletni kierownik CERT Polska, prezes Fundacji Bezpieczna Cyberprzestrzeń, współzałożyciel i wiceprezes ComCERT SA. Mirku, bardzo się cieszę, że możemy dzisiaj znów porozmawiać.

Mirosław Maj: Cześć. Dziękuję za zaproszenie.

Prowadzący: Słuchaj, we wszelakich wiadomościach widzimy masę informacji na temat obecnie trwającego konfliktu zbrojnego. Informacje te są głównie nastawione na działania grup zbrojnych oczywiście i na poczynania w tych aspektach dwóch stron. Wiemy również, że obok działań związanych ze stacjonarną armią, wojska, już ta bitwa dawno przeniosła się na inne płaszczyzny. Sankcje, media społecznościowe, a także działania bojowe bez konwencjonalnej broni, za to często równie niebezpieczna, a mianowicie wojna w cyberprzestrzeni. Jak w kilku zdaniach można podsumować dotychczasowe posunięcia zarówno z jednej, jak i drugiej strony?

Mirosław Maj: No one są bardzo ciekawe, bo myślę, że nie do końca spełniły się scenariusze, które były wskazywane, jako najbardziej prawdopodobne. Nieskromnie powiem, że trochę jakby się z nimi do końca nie zgadzałem i trochę wyszło tak na moje w tej dyskusji, dlatego że ja przewidywałem, że jeśli dojdzie do konfliktu kinetycznego, to cała warstwa cyber, to nie będzie ta warstwa, w której będziemy odnotowywali bardzo, bardzo niebezpieczne zdarzenia. No ja w ogóle nie wchodzę jakby w kwestie porównania do, do tego, co się dzieje w konflikcie kinetycznym, gdzie giną ludzie. Więc jakby tutaj nie powinniśmy sobie w ogóle, jakby w tę sferę moim zdaniem wchodzić. Dlatego, że no jest kilka przesłanek tu temu mówiących o tym, że to właśnie niedokładnie tak musi, tak musi być. I to się moim

zdaniem sprawdza, dlatego że oczywiście, mamy cały czas, codziennie są informacje mówiące o tym, jak wygląda ta wojna w warstwie cyber i wtedy myślę, że tutaj możemy jakby ograniczyć się do stwierdzenia, które generalnie krytykujemy, jeśli ktoś używa też od strony politycznej w odniesieniu do konfliktu, do wojny tak, czyli – konflikt, tak. Moim zdaniem w warstwie cyber jest to konflikt. W warstwie kinetycznej jest to wojna. Ten konflikt w warstwie cyber to, o czym wiemy i tutaj myślę, że jest takie bezpośrednie przełożenie, pochodną naszej, pochodną tej działalności i naszego jednocześnie spostrzegania tego, jak to wygląda jest to, jak kto informuje i o czym informuje, jeśli chodzi o działania w cyberprzestrzeni. Ja bym tutaj wyróżnił trzy główne podmioty albo kategorie podmiotów, które o tym mówią, no to mówimy po prostu o obydwu stronach jakby tej wojny, czyli o stronie ukraińskiej i o stronie rosyjskiej. No jeszcze mówimy o społeczności, niezależnie w tej chwili na tym etapie, na tym etapie dyskusji, jak ją oceniamy no, ale jednak jest społeczność, którą moglibyśmy jednym ogólnym stwierdzeniem ogarnąć, jako tak zwani anonimowi, anonymous words tak, czy różnie tam się na podgrupy jeszcze dzielą. I to są, i te działania wszystkie, bym powiedział one mają bardzo duże nasilenie. Natomiast one w mojej ocenie niewiele się różnią od tego, co my od lat już obserwujemy. Czyli mamy tutaj takie podstawowe wektory ataków. Na przykład w przypadku tej wojny, tego konfliktu w cyberprzestrzeni, jak ataki DDoS, jak związane głównie z blokowaniem serwisów, jak wycieki danych, czy w wyniku włamań do serwisów i jak, no próby, może tutaj akurat, może tutaj w tym wektorze ataku nastąpiło pewne nasilenie, próby związane z tym, żeby niszczyć na przykład dane, stąd te informacje o viperach [niepewne], które bym powiedział na potrzeby tego, tego starcia wyparły trochę powszechnie znane ransomware.

[00:05:21]

Mirosław Maj: Tak w skrócie, tak. A pewnie tutaj szczegółów jest cała masa jeszcze.

Prowadzący: Słuchaj, skoro już poruszyłeś kwestię Anonymous. Myślę, że warto byłoby tutaj troszeczkę dalej podrążyć temat, oficjalnie w stanie konfliktu oczywiście z Rosją. Tak przynajmniej ogłaszają aktywiści na, między innymi na swoich Twitterach. Na przestrzeni właśnie konfliktu nie działały już szereg rosyjskich witryn, usług, tak. Tutaj ciężko tak naprawdę ich wszystkich przytaczać. Ale czy z Twojego punktu widzenia mamy do czynienia z pospolitym ruszeniem podobnych grup, czyli mówiąc wprost, czy mamy do czynienia z większym odsetkiem właśnie incydentów aktywistów względem powiedzmy takich klasycznych hakerów nastawionych na zarobek przez niszczenie właśnie, czy szantaż danymi, czy wstrzymanie produkcji i tak dalej?

Mirosław Maj: No, oprussia, czyli operacja Rosja, którą anonimowi zapowiedzieli i realizują. No myślę, że tak historycznie, jeśli nie jest nawet, jeśli nie jest największą, no to myślę, że jest jedną z największych, jeżeli chodzi o właśnie takie zwarcie szyków tych anonimowych i prowadzenie

działalności. Więc to na pewno tak jest. Natomiast myślę, że skala tego rzeczywistego oddziaływania powinna być i myślę, że to jeszcze z czasem ktoś pokusi się, jeśli zbiera w tej chwili dane, tak. Bo tu pytanie, na ile będziemy mieć dostęp do, do tych danych. Jeżeli ktoś zbiera te dane i w przyszłości pokusi się o analizę tego, co tak naprawdę się stało, to dopiero będziemy mogli to ocenić no, bo tak na bieżąco widać, że niekoniecznie powinniśmy też, no jakby rzetelnie o tym rozmawiając, tak. Więc wiadomo, której stronie kibicujemy w tym, w tym wszystkim, ale, ale powinniśmy z pewnym dystansem patrzeć na te wszystkie ogłoszenia w sieci, co się dzieje, jakie ataki mają miejsce. No, bo podam tutaj najbardziej taki oczywisty przykład, który warto weryfikować. Można to robić dosyć prosto, czyli informacje o niedostępności pewnych serwisów w Internecie, związanych z działalnością Federacji Rosyjskiej, czy biznesem rosyjskim, czy przede wszystkim administracją rządową, służby FSB i tak dalej, i tak dalej. I te informacje mówiące o tym na przykład, że ta taka strona jakaś nie działa. Swego czasu, swoją drogą popularne było takie stwierdzenie, które teraz chyba w ogóle prawie tu nie jest używane, tak zwane tango down. To tango down, no odbywa się dosyć często, tylko zwracam uwagę, że jeżeli by przeprowadzić taką prostą bardzo analizę, jeżeli chodzi o analizę ruchu w sieci, no to może się okazać, że to tango down jest tylko z naszego punktu widzenia. Dlatego, że jeżeli zapuścimy proste sprawdzenie dostępności strony z serwisów, które są w różnych miejscach na świecie, no to wyraźnie zaczynamy widzieć to, że jednak Internet ma pewne granice. Od zawsze jest takie popularne stwierdzenie – w Internecie nie ma granic. No otóż, ja od dawna powtarzam, że jednak są. Może one nie są tak widoczne i trochę inne, inne reguły obowiązują, jeżeli chodzi o ich zarządzanie i przekraczanie ich, ale jednak są. I to widać, że mamy na przykład ogłoszenie o niedostępności przez kilka dni, tak było, niedostępności giełdy moskiewskiej. No i okazuje się, że jeżeli jak to zbadać, to, że strona tej giełdy moskiewskiej, już nie mówię o samych serwisach prawda, nie wiemy tego dokładnie, ale powiedzmy, że reprezentujemy tę informację poprzez fakt, czy strona jest dostępna, czy nie, no to okazuje się, że ta strona, my jej nie widzimy, ale ona z serwerów Federacji Rosyjskiej jest widoczna, czyli jest dostępna na przykład dla obywateli Federacji Rosyjskiej. Więc tak naprawdę mamy w tej chwili też i tutaj oczywiście zachodzą jakby zjawiska bym powiedział zarówno dezinformacji, jak i propagandy. No, bo to zależy jak to będziemy interpretowali i kto to, kto to robi, na ile celowo to robi, związane z tym, że no, to od zawsze od strony takiej rzetelnej analizy może troszeczkę inne, inne informacje przynieść, niż na pierwszy rzut oka się wydaje. Więc jest to na pewno na dużą skalę. No my nieprzypadkowo sami, jako Fundacja uruchomiliśmy taki codzienny zestaw informacji z tego frontu konfliktu pomiędzy, pomiędzy Rosją, a Ukrainą plus ci wszyscy, którzy wokół, wokół tego konfliktu się gromadzą i angażują się w niego, tak jak na przykład właśnie anonimowi.

[00:10:06]

Mirosław Maj: Tego jest bardzo dużo. Natomiast realne skutki i ocena nawet poszczególnych wszystkich tych ataków, no musi być rzetelna, tak. Jeżeli chcemy wyciągać z tego, robić jakieś wnioskowanie w oparciu o te informacje. A powinniśmy robić wnioskowanie w oparciu o te informacje.

Prowadzący: A z Twojej perspektywy, jak obecna sytuacja wpływa na kampanie cyberprzestępców, wykorzystujące po prostu tematykę wojenną na osoby, organizacje postronne, również z innych krajów. Czyli, co tutaj dużo mówić, stare metody infekcji, natomiast nowe tematy. Mówię tutaj o po prostu swojego rodzaju czy to naciągaczach, jak również o typowych kampaniach cyberprzestępców, którzy wykorzystują temat, aby skłonić nas do niebezpiecznych poczynań w Internecie.

Mirosław Maj: No tak, to jest ciekawy, ciekawy temat. Jest obserwowanych kilka nowych. Zawsze tak jest, cyberprzestępcy. Tutaj, jako ciekawostkę tylko można dodać takie zjawisko, że też pojawiają się takie kuriozalne ogłoszenia, jakby z tych grup przestępczych, że, no, na co dzień to my rozsyłamy spam. Ale teraz, no to wszystkie ręce na pokład, jeżeli chodzi o pomoc Ukrainie. Nie będziemy rozsyłali tego spamu, tylko walczyli z Rosją, więc wpłacajcie tutaj na nasze portfele bitcoinowe, żebyśmy nie musieli tego spamu rozsyłać. No mówię,no skutek…

Prowadzący: Sprawdzałeś może te portfele, czy rzeczywiście [niesłyszalne]?

Mirosław Maj: Tak, sprawdzałem, tam były, były podane dwa takie portfele przy jednej z takich akcji. Jedno było puste, na drugim były, było 14 wpłat, jakoś dziwnie wszystkie złożyły się, mimo że były teoretycznie różne, to na bardzo okrągłą sumę, którą w przeliczeniu na polskie po kursie z danego dnia wynosiła 10 000 złotych. Więc jakoś mam wrażenie, że to były jednak skoordynowane wpłaty pokazujące, że już inni wpłacają, więc może i ty wpłać. Taka jest moja interpretacja. Natomiast te groźniejsze i te, no tak jak mówię, powszechnie wykorzystywane sytuacje mówią no, nie tyle o nowych, tylko znowu o nasileniu. Bo są pewne elementy nowe, ja za chwilę o nich powiem. No, ale mamy tutaj takie wektory, w szczególności phishingowe ataku związane oczywiście z kwestią pomocy dla, dla Ukrainy. To zawsze tak było, wszystkie klęski humanitarne, takie katastrofy humanitarne związane były z tym, że wykorzystywano tutaj tą naturalną chęć dobrych ludzi, żeby pomagać i próbować ich naciągać, naciągać na to. Ale tutaj myślę, że warto zwrócić na dwa nowe wektory ataku i uczulić naszych słuchaczy, że no pojawiły się tego wektora, socjotechnicznego wektora, tak. I jeden z nich to jest powiązany z sankcjami. I taka informacja jak zwykle, która ma przestraszyć odbiorcę, że w związku z wprowadzonymi sankcjami, no ty tak gdzieś jesteś usytuowany w tym, w tym katalogu usług, że te sankcje w praktyce również dotyczą ciebie. No dzisiaj wiadomo, że jakby tego analizowanie dokładnie, z kim kapitałowo, kto jest powiązany, jak to się odbywa przy tak elastycznym przepływie dóbr, środków, usług w Internecie jest bardzo trudne i łatwo jakby w to, w to uwierzyć. I taka informacja, że musisz szybko coś zrobić, bo inaczej nie wiem, na przykład stracisz swoje pieniądze, bo właśnie okazuje

się, że jakiś tam bank korzysta z usług jeszcze innego banku, a ten jest objęty jakąś tam sankcją i tak dalej, i tak dalej. I trzeba po prostu coś zrobić. To jest jeden z takich wektorów ataku, na który trzeba bardzo uważać. Drugi natomiast jest taki trochę skierowany powiedzmy do warstwy organizacyjnie wyższej bym powiedział, nawet może, może nie dokładnie tam menadżerskiej, ale ludzi, którzy no może trochę z ciekawości, ale również być może z obowiązków służbowych, zawodowych, nie tylko tutaj w naszej branży ICT, tylko w ogóle w jakiejkolwiek branży, no może przesyłane są takie informacje o tym, że, no tutaj w wyniku wojny następuje, co jest oczywiste tak, trudno z tym kwestionować, do naruszenia łańcuchów dostaw i różnych ryzyk z tym związanych. No i trzeba sprawdzić znowu, czy czasami ty nie jesteś uzależniony i nie jesteś, czy to ryzyko w dużym stopniu ciebie nie dotyczy. No i tam gdzieś znowu jakieś formularze do sprawdzenia, do, no jakby dalej schemat jest ten sam, tak – albo link, albo plik do otwarcia no, ale jeszcze raz dalej schemat znowu jest ten sam, dochodzi do infekcji. Więc na pewno to wykorzystują, będą to wykorzystywali i musimy być przygotowani na to, że tutaj będzie tyle, już jest, a myślę, że jesteśmy tylko na początku okresu bardzo niekonwencjonalnych zdarzeń z punktu widzenia nie wiem, ekonomii, z różnych potencjalnych zagrożeń nowych, czy konieczności redefiniowania pewnych usług.

[00:15:20]

Mirosław Maj: Że no, ten pierwiastek, który jest potrzebny cyberprzestępcom do tego, żeby spróbować działać mocniej, na zasadzie wymyślić jakiś nowy wektor ataku, no to co chwilę będzie się pojawiał i to będzie im sprzyjało. I po prostu musimy być generalnie coraz bardziej czujni na najróżniejsze dziwne historie.

Prowadzący: Mirku, we wcześniejszym odcinku, który nagrywaliśmy razem dużo mówiłeś o grupach APT, w tym również oczywiście grupach z Rosji. Jak teraz wygląda ich aktywność i czy jest ukierunkowana tylko na stronę ukraińską, czy niekoniecznie?

Mirosław Maj: My nie mamy takich jasnych śladów w tej chwili działalności. Ja w ogóle, no jak to często się powtarza, obym się mylił, ale w ogóle uważam, że niestety my jesteśmy dopiero u progu, a może jeszcze chwilę poczekamy na to, że to się objawi z większą mocą, dlatego że sądzę, że albo w sposób strategiczny, albo poprzez fakt konieczności zaangażowania się w inne, w inne działania, te grupy w tej chwili nie przejawiają najwyższej aktywności. Być może niestety, jeśli, jeśli tak się stanie szykują się dopiero do bardziej poważnych operacji. Więc tak uważam, że w tej chwili jest. Pojawiają się oczywiście różne, różne informacje. Pojawiają się informacje na przykład o nowych, o nowych słabościach systemowych, których wykorzystanie się w sieci wzmaga tak, czyli może być powiązane na przykład z zupełnie z nowymi, przygotowywanymi na tę okazję sposobami działania i może dopiero się okazać za jakiś czas, że my całą naszą wiedzę, którą do tej pory mieliśmy na temat wektorów ataków, na temat

na przykład TTP, używanych przez te grupy rosyjskie, no to musimy, musimy odłożyć na półkę i być przygotowani na to, że mogą się pojawić zupełnie nowe. Więc taka praca trochę analityczna, researchowa w świecie na temat tego, co się wzmaga, a co nie, no to jest bardzo, bardzo ważna. Występują różne dziwne zjawiska, jak na przykład tygodniowe osłabienie skanowania portów związanych z usługą SSH, tak. Zupełnie jakby w prosty sposób niewytłumaczalne i wiadomo, że analitycy muszą dopiero zanurkować po prostu w te, w te pakiety i próbować rozwikłać, co się dzieje. Amerykańska CISA do właśnie wydała, właśnie wydała informacje na temat zdaje się 11 nowych CVE, które w szczególny sposób są wykorzystywane w ostatnim okresie. No i znowu może być tak, że one są powiązane z jakąś nową formą działalności, z nową sekwencją ataku, której do tej pory nie znaliśmy. Więc ogólnie rzecz biorąc, znowu troszeczkę wracając do tej rozmowy na temat tego, jak przewidywaliśmy, co się stanie, co się nie stanie, mi się wydaje, że w tej chwili jest tak, że te grupy, no na pewno nie zostały wysłane nigdzie na urlop, tak. One, one działają i działają może po części swoimi starymi sposobami, może troszeczkę więcej w tej chwili czasu spędzają na przygotowanie, strategiczne przygotowanie ataków. Może są na takim standby. A może już działają w sposób, który dopiero za jakiś czas będziemy potrafili zidentyfikować, że właśnie, właśnie działały. A może, oby tak nie było, są w stanie jakby przeglądu pełnego, sprawdzania tego, czy wcześniej zainstalowane mówiąc pewnie w pewien sposób taki metodyczny, bomby logiczne, nad którymi pracowali przez wiele, wiele lat. Bo wiemy o tym, że Federacja Rosyjska potrafi prowadzić w tym obszarze projekty wieloletnie, strategiczne projekty wieloletnie. To może właśnie w tej chwili jest okres jakby sprawdzania możliwości, mówiąc kolokwialnie, odpalenia tych ataków, oby tak nie było. Ale ja wolę tutaj trochę jakby wołać, wołać na alarm, bo wydaje mi się, że takie prawdopodobieństwo tego typu przebiegu sytuacji, takiego scenariusza, że za chwilę możemy mieć bardzo poważne problemy w cyberprzestrzeni. I co ciekawe, w mojej opinii mogą mieć bardziej sojusznicy Ukrainy, niż sama Ukraina, chociażby ze względu na to, że to może się okazać jedyny, jedyny sposób takiego odwetu za sankcje ekonomiczne. [00:20:00]

Mirosław Maj: No to, no to być może właśnie jesteśmy, jesteśmy narażeni na taki scenariusz i powinniśmy bardzo, bardzo się do tego przyłożyć, żeby być na to gotowi.

Prowadzący: A co z grupami z krajów takich, jak na przykład Chiny, w których władza, w teorii przynajmniej tak oficjalnie, nie zamierza na razie interweniować? Czy biorąc pod uwagę tego typu grupy również powinniśmy być tutaj bardziej wyczuleni?

Mirosław Maj: Uczciwie mówiąc do tej pory nie natrafiłem na szczególne informacje dotyczące aktywności chińskiej w cyberprzestrzeni. Myślę, że to jest, związanej z wojną tak, na, na, na Ukrainie. Myślę, że to jest gdzieś, no to oczywiście też jest kraj, który w sposób strategiczny i skoordynowany

działa, jeżeli chodzi o działalność polityczną, geopolityczną i również w cyberprzestrzeni. Myślę, że no tak jak Chiny są na pewnym, z jednej strony oczywiście tutaj pokazują, że jednak tutaj wspierają Federację Rosyjską. No, bo sam fakt nazywania wojny, wojny na Ukrainie, jako konflikt, że jest tam jakiś konflikt, no to, to już jest wyraźnie odbierane przez społeczność międzynarodową, jako ustawienie się po jednej stronie tej, jeżeli chodzi o przeciwników w tej wojnie, to myślę, że troszeczkę jest podobnie z tym, z tym obszarem, obszarem cyber, jak on dalej będzie rozwijany i czy Chińczycy bezpośrednio się zaangażują w ten konflikt cyberprzestrzeni. Ja bym zaryzykował stwierdzenie, że niekoniecznie, ale to nie oznacza, że oni będą nieaktywni. Ja myślę, że oni po prostu będą aktywni w obszarach powiązanych z realizacją swojej polityki przy okazji tego, co się dzieje na Ukrainie i przy okazji tego, co się dzieje w cyberprzestrzeni w związku z wojną na Ukrainie. Więc jeżeli sobie wymyślą to, że to jest czas realizacji swoich celów strategicznych, to ich działalność cyber będzie powiązana z tym. Zwracam też uwagę, że jakby takie najbardziej charakterystyczne wektory ataków i sposoby strategiczne działania Chińczyków w cyberprzestrzeni są mniej bym powiedział takie powiązane ze szczególnymi incydentami wpisanymi w oś czasu. One są bardziej strategiczne, bo na przykład powiązane z tym, że, że prowadzi się cyberszpiegostwo przez, operacjami wieloletnimi nawet, no albo kilkumiesięcznymi. Więc, więc one rzadziej mają taki charakter incydentalny, że właśnie nagle coś się stało i w związku z tym coś w cudzysłowiu. Oby dalej, w cudzysłowie, oby dalej w cudzysłowie wybuchło, niż to na przykład na jest przy okazji tego, co robią Rosjanie, którzy potrafili wyłączyć już dwukrotnie w poważny sposób prąd na, na Ukrainie i kilka jeszcze innych wyczynów tego typu mieli.

Prowadzący: Słuchaj, Charlie - CRP, co oznacza dla zwykłego, przeciętnego obywatela? Byliśmy bombardowani, chyba w sumie tak naprawdę dalej jesteśmy, wiadomościami o stanie wyjątkowym związanym ze znacznie większym prawdopodobieństwem ataków cyber. Natomiast wydaje mi się, że jednak było dosyć mało komunikatów informujących o powiedzmy konkretnych możliwych scenariuszach, czy możliwościach płynących za takim atakiem. Szczególnie dla ludzi spoza branży, jeżeli tak to mogę ująć.

Mirosław Maj: No myślę, że masz bardzo prawidłową obserwację tutaj. Bo ja właściwie troszeczkę też zadaję sobie to pytanie. Z jednej strony jeszcze niedawno trochę ekscytowaliśmy się wprowadzeniem stanu Bravo, który historycznie kilka razy został wprowadzony. W tej chwili mamy już, od zdaje się co najmniej dwóch tygodni, jeśli dobrze pamiętam i przedłużony jest w tej chwili zdaje się chyba do 15 marca stan Charlie – CRP, czyli to jest trzeci z czterech stanów alarmowych. Mamy jeszcze tylko jeden wyższy – Delta. I pytałeś o tak zwanego zwykłego obywatela. No formalnie rzecz biorąc, nic. Ja powiem nawet więcej, z punktu widzenia jakby obywatela, ale nie tylko, ale również na przykład firmy komercyjnej, która prowadzi bardzo zaawansowaną działalność w cyberprzestrzeni, również nic.

Dlatego że, dlatego że, że ten stopień alarmowy dotyczy firm administracji publicznej i dla nich, dla nich jest wprowadzony. Oczywiście on się przenosi w praktyce w szczególności na tych, którzy dostarczają usługi dla tej administracji. Ale myślę i takie głosy się też pojawiają, a ja się pod nimi podpisuję, że być może ta sytuacja, którą teraz obserwujemy, to jest dobra przyczyna do dyskusji. [00:25:10]

Mirosław Maj: A może tutaj w ogóle nie za bardzo mamy teraz czas na dyskusję, tylko na bardzo konkretne działania, dlatego żeby konsekwencje wprowadzenia takiego stopnia alarmowego być może nie wiem, od któregoś stopnia, a może dla wszystkich, nie dotyczyły tylko i wyłącznie administracji publicznej, ale dotyczyło też innych firm. No mamy na przykład w Ustawie o krajowym systemie cyberbezpieczeństwa takie określenie status podmiotu, jako operator usług kluczowych, no więc, więc trochę niezrozumiałe jest pewnie dla wielu, dlaczego akurat Charlie – CRP dotyczy tylko administracji publicznej, a nie dotyczy na przykład takich podmiotów. Bo, bo wiemy, że no tutaj w scenariuszach, które snujemy, tych najbardziej groźnych, że to właśnie konsekwencje ataków na tego typu podmioty mogą być dla nas najgroźniejsze. No i, i teraz, co tak naprawdę się dzieje po wprowadzeniu tego stopnia alarmowego? No myślę, że dzieje się z punktu widzenia pewnej organizacji, przede wszystkim najwięcej się dzieje z punktu widzenia pewnej organizacji systemu obsługi systemu cyberbezpieczeństwa poszczególnych podmiotów, współpracy ewentualnie pomiędzy nimi, tak. To myślę, że no, wprowadzenie większej gotowości, dostępności zasobów, ludzi, którzy mają reagować i tak dalej. To się na pewno dzieje i tutaj to jakby podnosi na wyższy poziom. Natomiast myślę, że trochę mało się dzieje i może to też jest dobry, dobry punkt do dyskusji i do zmiany w kontekście konieczności jakby podkręcenia śrubki technicznej, technicznie bym powiedział, tak. Czyli jeżeli mamy tutaj informację o możliwym bezpośrednim ataku na nasze kluczowe zasoby, to być może powinien być wypracowany taki model, że każdy z takich podmiotów, którego później dotyczy stopień alarmowy ma też swoją opcję konfiguracji, tak już powiem ogólnie, na poszczególne stany, tak. Czyli schodząc jakby do kwestii konkretnego, konkretnego urządzenia, to może być tak, że mamy specjalny zestaw reguł bardzo restrykcyjnych na firewallu i uruchamiamy je tylko, dlatego że ktoś wprowadził bardzo wysoki stopień, bardzo wysoki stopień alarmowy, i powinniśmy go po prostu wykorzystać w tym, w tym momencie. Myślę, że to by się też przydało tak, bo my do końca, mówię, jak się zorganizować lepiej, to już wiemy tak, bo to gdzieś tam mówiłem, te dyżury 24h i tak dalej, i tak dalej, lepsza dostępność ludzi, ale co to oznacza, co my tak naprawdę powinniśmy zrobić w sieci, w konfiguracji sieci, urządzeń, no to to, to raz, że w ogóle świadomość tego nie jest oczywista. Myślę, że niektórzy dopiero dochodzą po jakimś czasie, no dobra, już mamy te dyżury 24 na dobę, ale tak naprawdę, czy my gdzieś tam lepiej zabezpieczyliśmy

naszą sieć i nasze urządzenia, nasze serwisy, usługi, tak? I później się dopiero za to, jakby ta dyskusja rozpoczyna.

Prowadzący: No tak. To, że ktoś jest dostępny na miejscu 24 na dobę tak, to nie znaczy, że infrastruktura może być przygotowana i czy nie będzie scenariusza, że te osoby, które są na miejscu, to po prostu rozłożą rączki, i będą się przyglądały bezczynnie. Bo tak naprawdę nie będzie, co zrobić.

Mirosław Maj: Nie powiem, że gorzej, tak. No, bo trudno, trudno tutaj jakby forsować taką tezę, że jak będziemy mieli dyżur dłużej, niż normalnie, to będzie gorzej. No, ale pamiętajmy, że w trakcie takiego, żeby mieć dyżur dłużej, no to musimy wprowadzić nie wiem, no być może nowe osoby do tego cyklu dyżurów i te osoby mogą być akurat mniej doświadczone. I wtedy, no nie wiem, właśnie znowu osobowo organizacyjnie mamy takie poczucie spełnionego zadania, a jakościowo, a jakościowo to już wcale niekoniecznie musi wyglądać dobrze, więc to też jest ważne, ważny element. Może to jest moment taki, w którym trzeba przemyśleć na nowo ogólnie taką strategię nie wiem wsparcia na przykład przy takich kryzysowych sytuacjach tak, co trochę się dzieje, aczkolwiek tutaj też troszeczkę jakby krytycznie na to patrzę, bo obserwuje się bardzo duże zainteresowanie tym, że takimi rozmowami na temat – jak poprawić nasze, nasz poziom cyberbezpieczeństwa. Dlatego niestety w większości przypadków to są takie chyba, ja to określam, jako uspokojenie, jakby swoich nie wiem czy wyrzutów sumienia, że nie wszystko zrobiłem, albo spróbowanie takiego – tak, coś zrobiłem. Natomiast, no powiedzmy sobie szczerze, no dyskusja o tym, że trzeba poprawić poziom cyberbezpieczeństwa, bo stało się groźniej nie poprawia samo w sobie poziomu cyberbezpieczeństwa, tylko po prostu trzeba podjąć, podjąć działania.

[00:30:05]

Mirosław Maj: Więc, no pytanie, czy to się skończyło na dyskusji i później tłumaczeniem, no już podjęliśmy rozmowy, czy naprawdę coś, ktoś zrobił. I moje obserwacje na razie są krytyczne, niewielu dużo zrobiło w tym czasie i to jest akurat moim zdaniem, niepokojące.

Prowadzący: Słuchaj, klika razy już podczas naszej rozmowy dzisiejszej poruszyliśmy delikatnie temat infrastruktury krytycznej. Więc może pozostańmy jeszcze chwileczkę przy tym. Jak operatorzy infrastruktury krytycznej przygotowują się na odparcie ataków? Czy będziemy świadkami sprawdzianu Dyrektywy NIS w praktyce? Takiej dojrzałości tejże dyrektywy i właśnie przygotowania tychże instytucji?

Mirosław Maj: Z tą Dyrektywą NIS to jest troszeczkę tak, jak z tą naszą dyskusją o stopniach alarmowych. Bo ona też, no dla przypomnienia, no Dyrektywa NIS w naszych warunkach polskich ma swoją materializację w postaci Ustawy o krajowym systemie cyberbezpieczeństwa, która została wprowadzona, dlatego żebyśmy spełnili te wszystkie, wszystkie wymagania. No i znowu jest tak, że

troszeczkę tak, jak mówię, trochę podobnie, jak z tymi stopniami alarmowymi. Mamy tam zaproponowane, wymyślone, mamy gdzieś tam swoje własne też autorskie pomysły pod tytułem czy CSIRTy krajowe, gdzie to nie jest jakby zapis Dyrektywy, Dyrektywy NIS. Bo Dyrektywa NIS mówi o csircie krajowym. Nie mówię o tym, że nie można mieć więcej, więc my mamy akurat. Więc to jest nie jeden do jeden tak jak mówimy często GDPR i RODO prawda, że to jest jakby rozporządzenie, więc mamy jeden do jeden, tylko mamy swoją implementację Dyrektywy NIS. I ona znowu w warstwie organizacyjnej zaproponuje pewien model. Ten model generalnie polega na tym, że mamy na górze pełnomocnika, mamy trzy, operacyjnie tak przede wszystkim mówię, chociaż no pełnomocnik nie do końca jest operacyjnym ciałem, ale mamy tego pełnomocnika do spraw rządu, do spraw cyberbezpieczeństwa. Mamy csirty krajowe, mamy albo nie mamy, bo mamy do tej pory jeden, chociaż moglibyśmy mieć kilkanaście, a mamy tylko jeden csirt sektorowy, czyli csirt KNF Komisji Nadzoru Finansowego dla sektora finansowego, czyli te csirty sektorowe. I mamy, i mamy jeszcze, no tych, którzy poszczególnych operatorów usług kluczowych powinni zorganizować ten system, no czytaj mieć co najmniej jakieś zespoły tak, które tym się zajmują. Znowuż tutaj tą warstę organizacyjną w jakiś sposób mamy, co jest bardzo ważne, bo ja to, żeby było jasne, akurat tutaj to moja opowieść o tym nie ma charakteru krytycznego tylko raczej pozytywny, że bardzo dobrze, że tak jest. Natomiast, bo od czegoś trzeba zacząć, natomiast nie mamy w tej chwili żadnego systemu prostego sprawdzania takiego praktycznego, ani deklaracyjnego tego, jak to wygląda w praktyce, na ile my poprawiliśmy swój poziom cyberbezpieczeństwa. Czyli krótko mówiąc nie mamy benchmarku dla tego całego systemu. Myślę, że to jest coś, nad czym warto by było popracować. I no jest trochę wzorców, tak jak Amerykanie potrafią to liczbowo wręcz przedstawić, który z sektorów cyberbezpieczeństwa jest na jakim poziomie, ile tam punktów dostaje, dlaczego nie? Można by było i takie coś zrobić. To oczywiście wszystko będzie miało tam swoje jakieś ograniczenia i nie będzie idealnym obrazem, ale będzie lepszym niż mamy to, co w tej chwili jest, bo tak naprawdę my do końca tego nie wiemy. Wydaje się też, że sporo tych działań, które są realizowane w ramach KSC w mojej ocenie mają za bardzo charakter, no nie chcę tego nazywać w jakiś sposób tajny, czy tam poufny tak, bo to chyba nie do końca o to chodzi. Tylko myślę, że one są za mało widoczne. Wiemy, że w tej chwili odbywa na przykład się jakaś koordynacja, koordynacja w poszczególnych, przynajmniej próby w niektórych sektorach, albo gdzieś tam na poziomie krajowym. Ale no mówiąc szczerze zupełnie tego nie za bardzo widać na zewnątrz, tak. Bo jak byśmy sobie prześledzili tę komunikację, te alerty, które wychodzą ze strony tych wspomnianych tutaj różnych instytucji, to tego nie ma dużo. To okazuje się, że tego nie ma dużo. Tutaj może akurat wracając trochę do opowieści na temat csirtów sektorowych, no to przykład akurat może csirt KNF pokazuje, że chyba

jest szansa na to, żeby taki bardziej operacyjny, koordynujący charakter spełniały takie csirty, jeśli by powstały, tak. No one, po prostu one nie powstały, tak.

[00:35:01]

Mirosław Maj: Jedna jaskółka wiosny nie czyni. Ja osobiście uważam, żewłaściwie to powinna być mocna rekomendacja dla tych, którzy decydują o tym, jak to w Polsce jest poukładane, żebyśmy w trybie niemalże natychmiastowym takie zespoły powołali, albo bardzo wyraźne powiedzieli, kto funkcje tego typu, tego typu zespołu pełni dla danego sektora. To tylko podpowiem tyle, że w nowelizacji, która już w tej chwili nie wiem, chyba blisko 2 lata gdzieś mieli w machinach rządowych, jeżeli chodzi o Ustawę o krajowym systemie cyberbezpieczeństwa w tej nowelizacji. Akurat csirty sektorowe są podmiotami obowiązkowymi dla poszczególnych sektorów. No, więc jakby tu intencja jest jasna. Jak rozumiem to, że tak się stało, taki jest zapis i taka propozycja w tej nowelizacji to też jest wynik pewnej analizy i jasności braku wątpliwości, co do tego, że tak powinno być. Ale mamy tylko, jeszcze raz powtarzam, tylko jeden crist sektorowy. Więc mamy no jakby przesłankę nawet, już wynikającą z wcześniejszych analiz, że to jest coś, czego potrzebujemy. I w tej chwili mamy już zapis o tym, że takie csirty mogą powstawać, ale nie są obowiązkowe, dlatego mamy tylko jeden. Więc na bazie obecnych przepisów można by było bardzo mocne działania katalizujące ten proces podjąć. I takie zespoły w mojej ocenie powinny powstać jak najszybciej.

Prowadzący: A który sektor, biorąc pod uwagę infrastrukturę krytyczną i patrząc przez pryzmat Twojej wiedzy, doświadczenia, ale również no, obecnych działań, byłby takim najbardziej łakomym kąskiem dla, dla napastników i mógłby spowodować taki, tak naprawdę największy cios?

Mirosław Maj: No, tutaj myślę, że to jest oczywistym, najbardziej pożądanym celem dla takich działań to są dwa sektory. To jest sektor finansowy i sektor energetyczny. Szczęśliwie jest tak, że w tych całych opowieściach negatywnych, tam gdzie negatywnie oceniamy sytuację, no to akurat tutaj pewnie byśmy szczęśliwie mogli się przyczepiać jak najmniej, dlatego że sektor finansowy, w którym, jak ja to mówię, jest najkrótsza droga pomiędzy atakiem, a realnymi stratami wymiernymi, jak rzadko, w którym sektorze, tak. Po prostu włamanie na konto, włamanie do serwera, no wiąże się właściwie bezpośrednio, natychmiastowo z utratą takich i takich środków. Więc ten sektor już zrozumiał wiele, wiele lat temu, jak ważne jest cyberbezpieczeństwo i zainwestował bezsprzecznie najwięcej, chcąc nie chcąc, tak. No, bo to jest, tam w zrozumieniu, że to jest fragment biznesu, że to nie jest wydawanie pieniędzy, to nie jest liczenie, jako, jako koszt taki niezrozumiały, tylko to jest po prostu praca, inwestycja w to, inwestycja w cyberbezpieczeństwo jest, jest pracą na rzecz lepszego wyniku finansowego, lepszego świadczenia usług i tak dalej, i tak dalej. Takie, takie przekładnie zrozumienia w innych sektorach występują bardzo, bardzo rzadko. Więc drugi sektor, akurat energetyczny, na

szczęście troszeczkę ma, no inne, nie ma takiej, takiej, takiego przełożenia, o którym tutaj sobie mówiliśmy. Natomiast myślę, że z latami, w kilku ostatnich latach zdecydowanie wzrosło to, ta świadomość ryzyka związanego z działalnością tego, tego sektora. Pojawiły się zespoły, pojawili się ludzie, którzy rozumieją, że ciągłość działania usług kluczowych, związanych z szeroko rozumianą energetyką, nie tylko elektroenergetyką, tylko szeroko rozumianą. To bezpieczeństwo innych mediów, innych, innych rzeczy, jeżeli chodzi o zaopatrzenie i świadczenie usług, że, że to jest tak powiązane z cyberbezpieczeństwem, że na szczęście, gdzie w wielu miejscach już zostało to zrozumiane, zostały odblokowane środki na to i rzeczy się dzieją. To, to oczywiście też są sektory, które ze względu na przykład na funkcjonowanie spółek Skarbu Państwa bardziej są narażone na różne turbulencje, jeżeli chodzi o organizację tego, bo zmieniają się władze w tych spółkach, przychodzą nowi ludzie, oni wprowadzają swoich ludzi, swoich szefów różnych departamentów. To oczywiście też jakby departament, czy cała, cała struktura organizacyjna związana z cyberbezpieczeństwem nie jest wyjęta z tych procesów, z tych zjawisk.

[00:40:00]

Mirosław Maj: Więc tam, tam oczywiście pewne zamieszanie od czasu do czasu przychodzi. No przełóżmy sobie je wyżej, tak. No sam fakt, że mieliśmy Ministerstwo Energii, już nie mamy Ministerstwa Energii. Teraz mamy Ministerstwo Klimatu, w którym to się zajmują, czy jeszcze przy okazji zawirowania wokół Ministerstwa Cyfryzacji. No to wszystko sprawiało, że im bliżej to jest polityki, tym to ryzyko jakby tych turbulencji i oddziaływania ich na poziom cyberbezpieczeństwa, jeżeli chodzi o struktury organizacyjne no, które przecież i tak muszą koniec końca zadbać o to bezpieczeństwo techniczne, no to, to ryzyko jest większe, i tam, tam czasami to jest trochę utrudnione. Ale wracając jakby do podstawowego pytania, to na pewno są dwa sektory, które w szczególności mogą być celem ataków. Ale przecież to mogą być jeszcze inne, w których właściwie do tej pory niewiele słyszeliśmy o tym, żeby ktoś za bardzo się cyberbezpieczeństwem zajmował. To mogą być sektor związany na przykład z transportem tak, no to dzisiaj wiemy, jakie, jakie to jest kluczowe, czy ze służbą zdrowia też może być podobnie. Więc, no wystarczy nawet, nawet te dwa przykłady. Każdy z nas dzisiaj rozumie, jak krytyczne dla funkcjonowania państwa, życia obywateli są to sektory. No, a nie możemy absolutnie tutaj sobie snuć długich opowieści, jak to kiedyś tam było, jak doszło do takiego momentu w historii, jaki mamy dzisiaj, że zarówno sektor finansowy i sektor energetyczny to już coś zrobiły, tak. No, bo tam jeszcze takiej historii nie ma. Tam, tam po prostu takie rzeczy się nie wydarzyły. I tutaj znowu musimy pewnie mocniej przyłożyć takie działania natychmiastowe.

Prowadzący: Słuchaj, to teraz, teraz inny temat – łączność. Czyli jeden z kluczowych elementów i myślę, że jej przerwanie podczas działań wojennych, może odnieść krytyczne skutki. Myślę, że przypuszczasz,

o co chciałbym zapytać, a dokładnie o projekt Elona Musca i Starlink tak, dostarczenie terminali na stronę ukraińską. Jak dużą rolę mają tego typu systemy, biorąc pod uwagę tego typu w tym momencie sprawy wojenne?

Mirosław Maj: No, to można było jakby zacząć, może paradoksalnie skończyć powiedzeniem wojskowym, że – łączność jest najważniejsza, tak. Takie jest jedno z powiedzeń wojskowych, że łączność jest najważniejsza. I tutaj, zresztą, co ciekawe, jeden jakby z interpretacji sytuacji, od której zaczęliśmy tak, że ta wojna na Ukrainie wcale nie wiąże się z jakimś takim totalnym zaatakowaniem serwisów infrastruktury ICT i pozbawieniem dostępu na przykład chociażby do Internetu. To jedna z interpretacji mówi o tym, że no na przykład Rosjanie tego nie robią, dlatego że sami też tego potrzebują, że korzystają z tego, zarówno w sposób czynny, jak i bierny. No czynny, bo potrzebują, a niektórzy też mówią o tym, że też zakładają, że będą potrzebowali do tego, żeby sprawnie, sprawnie korzystać z tego w momencie wygranej. Oby do tego nie doszło no, ale to jest jedna z interpretacji. A drugie, taki sposób bardziej, bardziej bierny, że to jest też płaszczyzna, to jest ta sfera pozyskiwania informacji wywiadowczej, prawda. Możesz ją pozyskiwać na przykład dotyczącą tego, gdzie, kto się znajduje, co robi, no każdą, każdą jakby z sekcji bezpieczeństwa możesz tutaj próbować atakować, ale głównie chodzi o integralność i poufność danych. No to, to oczywiście też może być wykorzystywane i dlatego, dlatego nie jest, nie jest atakowane. Więc wracając do tego projektu Elona Musca, to oczywiście było absolutnie w pierwszych dniach, jeżeli dobrze pamiętam, chyba drugi czy trzeci dzień, gdzie minister Ukrainy do spraw transformacji cyfrowej chyba, usług cyfrowych, tak mniej więcej to się nazywa zaapelował na Twitterze do Elona Muska, żeby udostępnił Starlinka na terenie Ukrainy. I rzeczywiście tak się stało, no temu towarzyszyły, towarzyszą w tej chwili różne informacje o tym, że to nie jest takie proste prawda, że na przykład ten tak zorganizowany ruch sieciowy, ten dostęp do Internetu można zakłócać, tak. Tutaj mamy zjawiska jammingu radiowego. No i można je nawet niszczyć tak naprawdę pewnie jakby, jakby się chciało. Więc z tą dostępnością, no może, z tą dostępnością też jest różnie. Ale wszelkie działania tego typu, no z pewnością pokazują, że dzisiaj jest tak, że jakby ta platforma sieciowa, jakby w ogóle dostarczania, realizacji najróżniejszych usług w ogóle IT tak, szeroko ICT, nawet nie mówimy teraz o bezpieczeństwie stricte, no stała się tak czołowym elementem infrastruktury.

[00:45:21]

Mirosław Maj: No jak byśmy porównywali niemalże, może to za daleko idące, ale nie aż tak strasznie daleko, porównanie jest takie, to tak jakby, dlatego że jakby Rosjanie zaczęli niszczyć drogi tak, zanim sami na nie wjadą. No nie miałoby to kompletnie sensu, bo chcą je wykorzystać i tylko, dlatego że są ukraińskie. No być może, jeżeli by chodziło o zniszczenie totalne, tak i zabranie się, i wrócenie do

Moskwy, no to być może tak by zrobili. Jednym nalotem dywanowym mogliby zniszczyć, ale nie o to w tej wojnie chodzi. I myślę, że podobnie trochę jest z usługami cyfrowymi i z tą dostępnością usług. Ona jest po prostu w tej chwili pewnym podłożem do realizacji tak wielu różnych rzeczy, że no jakby jej niszczenie niesie ze sobą duże, duże ryzyko i myślę, że żadna ze stron nie jest tym do końca zainteresowana. Lokalnie oczywiście to się dzieje, bo słyszeliśmy już o takich rzeczach, że gdzieś tam nie ma dostępu na przykład do sieci telefonii komórkowej. No tylko, że no, tak jak obserwujemy, co się dzieje na Ukrainie, jeżeli chodzi o tę wojnę i zniszczenia, które na co dzień obserwujemy w telewizji, no to trudno sobie wyobrazić, że jakimś cudem to wszystko omija infrastrukturę usług cyfrowych, tak. To są po prostu przecież również maszty telekomunikacyjne i najróżniejsze części infrastruktury związane nie wiem, nawet jak coś jest w ziemi, no to przecież to też widzimy, że ta ziemia jest zaorana w wielu miejscach w wyniku tej wojny i bombardowania na przykład. Więc to po prostu musi się dziać. No trudno sobie wyobrazić, że takich efektów nie będzie, ale myślę, że ta wojna pokazuje, że dzisiaj Internet, sieć w ogóle telekomunikacyjna stała się tak ważnym elementem infrastruktury, że podjęcie, jeszcze raz, podjęcie jakichś działań destrukcyjnych wobec niej, no jest chyba dopiero drugim priorytetem. Pierwszym to jest jakby chęć panowania nad tym.

Prowadzący: Jeżeli chodzi o sankcje cyfrowe skierowane na Rosję, jakie w chwili obecnej są aktywne, a jakie jeszcze mogą zostać nałożone? Co to może oznaczać dla obywateli Rosji?

Mirosław Maj: No, jeżeli chodzi o sankcje to słyszymy, codziennie właściwie docierają, chociaż pewnie większość to już to zrobiła, więc jeżeli chodzi o jakieś tam pareto, to pewnie za chwilę je osiągniemy, jeżeli chodzi o to, co jest dostępne dla Rosji, dla obywateli. No firma za firmą, usługa za usługą są wycofywane, wielkie, wielkie koncerny międzynarodowe IT się wycofują ze swoimi usługami, wielkie firmy consultingowe. Niektórzy, no jakby odcinają się od tych, od tych usług. No tutaj cały czas jest tam rozmowa, znowu też trochę taka, w której nie ma łatwych odpowiedzi na temat tego, na ile wyłączać na przykład dostępność usług związanych z portalami społecznościowymi. No, bo niektórzy słusznie pewnie zauważają, że być może jest to jeden z nielicznych sposobów próby dotarcia z prawdą do Rosjan. No to akurat widać pewnie, w których momentach to jest tak postrzegane, bo wtedy akurat, no władze rosyjskie wkraczają do akcji i same, same się odcinają od Internetu. Więc tych sankcji jest cała masa. No olbrzymie niektóre, bardzo dotkliwe. Ciekawe, jak których konsekwencji pewnie jeszcze w tej chwili nie jesteśmy w stanie do końca oszacować. No, ale jeżeli wycofuje się ze wszystkim praktycznie taki, taki gigant, jak firma Microsoft, no to możemy sobie tylko wyobrazić. To oczywiście nie jest też takie wszystko bardzo łatwe, bo to nie jest tak, że na przykład już jak trzymając się tego przykładu Microsoft, albo z innych tak, no nie wiem, [niesłyszalne] chodzi o działalność licencyjną się wycofa i nagle to przestaje wszystko działać. No, bo już dochodzą do nas informacje o tym, że Federacja

Rosyjska planuje takie przedsięwzięcie pod tytułem – wyluzowanie, jeżeli chodzi o pewne restrykcje, legalizuje piractwo na obszarze Federacji Rosyjskiej. Ale z punktu widzenia jakby ich sytuacji trudno się dziwić tym, absolutnie nie można ich popierać tak, ale trudno się im dziwić, bo to jest kwestia chęci utrzymania jakby ciągłości działania właśnie w obszarze ICT, gdzie no bez tego byłoby to bardzo trudne. [00:50:06]

Mirosław Maj: Jeśli temu wszystkiemu towarzyszą działania na poziomie, na takim trochę bliższym aplikacyjnym, że próby utrzymania, wyparcia, szybkiego zastąpienia pewnych usług, od których było się uzależnionym swoimi rozwiązaniami, a może jakimiś partnerskimi z kimś, z kimś innym, no to to wszystko będzie miało takie skutki jak, odwrotnie proporcjonalne do tego jak skuteczne są te działania zastępcze. I to myślę, że dopiero będziemy obserwowali. I to nie ma, nie ma jasnej na to odpowiedzi, i nie ma tutaj też takiego. My popieramy oczywiście te sankcje, czytamy o nich, popieramy je, ale ja bym przestrzegał tu przed takim hura optymizmem, bo teraz wszyscy się wycofają i na pewno za chwilę żaden komputer i nic nie będzie działało w Rosji, i nic tam nie będzie można zrobić. No tak nie będzie. Pytanie tylko, w jakim stopniu i na ile będzie to dotyczyło jakby usług, usług kluczowych. Więc te sankcje, te sankcje będą narastały. Ja myślę, że jeżeli chodzi o sankcje te, jak pewnie każde inne, ale tutaj te, te związane z cyfrowymi usługami, no to my ich prawdziwe skutki dopiero będziemy potrafili oszacować za jakiś czas. Ja myślę, że one również będą mocno powiązane z tym, na ile ci wszyscy, którzy w tej chwili wprowadzają te sankcje, będą w nich konsekwentni. No nieraz to są takie działania natury fizycznej tak no, jeżeli ktoś likwiduje wszystkie swoje biura i wynosi się, i zwalnia kilka tysięcy ludzi, bo takie historie są też, jeżeli chodzi o duże firmy amerykańskie, na przykład consultingowe, no to wiadomo, że, przypuszczam, że to jest ruch wieloletni tak, że w ogóle ryzyko działania w tym obszarze plus jakby ryzyko objęcia sankcjami, dlatego że się gdzieś zarabia pieniądze na tym obszarze. No to, to w tym firmach akurat takie strategiczne myślenie zawsze występowało, bo one z tego żyją. I one po prostu przypuszczam, że podjęły taką decyzję już na długi czas i to tak będzie. Natomiast to wszystko, co można łatwo odtworzyć, zdalnie odtworzyć, no to, to może się zmieniać i zobaczymy po prostu jak Zachód będzie konsekwentny w utrzymywaniu, a być może wprowadzaniu nowych, nowych sankcji. Myślę, że to jest dosyć, tutaj nie widzę jakiejś strasznie dużego, dużej różnicy pomiędzy tym, jak jeżeli chodzi o te tradycyjne różne, głównie ekonomiczne sankcje, a te. Aczkolwiek może ciekawy jest wątek, bo on jest właściwie taki niezauważalny i w niewielkim stopniu, ja przynajmniej to obserwuję, na ile w tej całej szeroko rozumianej branży ICT ten komponent cyberbezpieczeństwo będzie w tym uczestniczył. Bo tutaj znowuż mamy taką tricking [niepewne] situation, jak to się mówi, w którym, no jest dyskusja też w społeczności międzynarodowej związanej z organizacjami zaangażowanymi na przykład w reagowanie na incydenty. Na ile znowuż nie są to organizacje, które mają pewnego rodzaju

misyjną działalność związaną z tym, że, może to za daleko idące, ale żeby troszeczkę wyobraźni, nie chciałbym, żeby się przywiązywać mocno do tego porównania, ale to gdzieś tam na wyobraźnię może zadziałać. No tak, jak nie wiem, działamy na rzecz podtrzymania takich kluczowych usług związanych dla obywateli. Na przykład związanych ze służbą zdrowia i to powinno wykraczać poza, poza na jakiekolwiek dyskusje, czy tutaj w to ingerować, czy nie. No to, to, to widzimy nawet w zapisach związanych z prawem międzynarodowym, albo tym, co od razu sprawiło, że Rosja jest na liście, od razu została podana do, wszczęte postępowania związane jakby z tymi zbrodniami, zbrodniami przeciwko ludności cywilnej. No to, to są gdzieś tam tego typu rozważania. Mówię oczywiście proportions gardees, jak najbardziej dla tego, ale tutaj ten świat cyberbezpieczeństwa ma, trochę ma orzech do zgryzienia. Ja akurat uważam, że on w większości nie jest aż tak przywiązany do tego, co powinno się chronić, niezależnie od wszystkiego, że też powinno go stać na, być stać na to, żeby w bardzo taki stanowczy sposób pokazać, że nie zgadza się na to, żeby w jakikolwiek sposób funkcjonować w strukturach, gdzie podmioty, a w szczególności te podmioty powiązane bezpośrednio z administracją rządową rosyjską funkcjonują, żeby jakiekolwiek formy współpracy z nimi prowadzić.

[00:55:01]

Prowadzący: A jak oceniasz informacje, które są obserwowane, jeżeli chodzi o projekt Runet, czy rzeczywistym jest scenariusz, gdzie Rosja może występować, jako swojego rodzaju taka wyspa na morzu, odseparowana tak naprawdę od reszty świata?

Mirosław Maj: Ja akurat przyłączę się do tych głosów, które mówią o tym, że jest planowana realizacja scenariusza odłączenia się, takiego umownego, tak. Bo dzisiaj byśmy musieli pewnie przeprowadzić długą dyskusję również o podłożu technicznym, na ile to jest w ogóle możliwe. Ale powiedzmy, no na tyle, na ile jest możliwe, takiego odłączenia się, odseparowania się od sieci, od sieci światowej Internet. I te działania, które obserwujemy, które niektórzy interpretują, jako właśnie przygotowanie do tego, no to są raczej bym powiedział przygotowania do tego, żeby ograniczać różne, negatywne skutki, no na przykład sankcji, albo ataków, ale nie, żeby samemu się odłączać. Odłączać się być może gdzieś tam wycinkowo tak, bo samemu się często podejmuje taką, taką decyzję, albo będziemy odłączani. Bo tak jak byśmy sobie gdzieś to przeanalizowali, no to nawet, jeżeli ktoś takiego pstryczka, jeśli w ogóle jest taki pstryczek pod tytułem „odłączamy się", powiedzmy, że on jest i nawet, jeżeli go nikt nie uruchomił, no to, to i tak w praktyce takie odłączanie poprzez nawet w warstwie aplikacyjnej, no się odbywa. Bo tutaj już w czasie tej dyskusji podaliśmy ileś przykładów tego, że to jest niedostępne, tamto jest niedostępne, no to, że pewne strony tylko w Federacji Rosyjskiej są dostępne, no to oznacza też, że trzeba by gdzieś je odseparować, gdzieś jakiś [niesłyszalne] wprowadzić. Więc na pewno elementy takiego uniezależnienia się od sieci Internet zostały uruchomione. Zresztą bardzo dobrze wiemy o tym,

że w przeszłości były takie testy. No, w kilku ostatnich latach już co najmniej kilka razy słyszeliśmy o różnych informacjach, o tym, że właśnie takie testy niezależności funkcjonowania w stosunku do Internetu światowego są przeprowadzane. I na pewno Rosja jest w gronie tych państw, które pewnie są najlepiej przygotowane do tego, tak. To nie znaczy, że idealnie, ale najlepiej myślę, że obok Chin czy Iranu to, czy wszędzie to albo przez chwilę, albo przez dłuższy czas tak, jak Chiny, czyli wielki firewall ćwiczone jest przez długi czas, albo incydentalnie tak, jak to bywało w Iranie. Natomiast no ten pstryczek nikt go nie naciśnie, dlatego że, no chyba raz, że no chyba raz, że to do końca nie będzie takiej trochę potrzeby. A po drugie, że no jest myślę, że sporo takich linków, które by sprawiło, że nawet z punktu widzenia tego, który to świadomie zrobił, to więcej mogłoby być strat, niż korzyści z takiego czegoś. Myślę, że akurat w dziedzinie, no jakby przekręcenia tego pstryczka po to, żeby uniknąć, uniknąć ataków, no to Rosja być może jest gotowa do takiego starcia, tak. Ona nie mówię, że się nie boi tak, ale akurat to, to jest pewnie jeden z nielicznych obszarów dzisiaj, w którym jest w stanie na przykład rywalizować ze Stanami Zjednoczonymi. Nie wiemy tak naprawdę, obyśmy nie musieli sprawdzać, który z tych potencjałów jest, jest wyższy. Ale mówimy tutaj o dwóch państwach, które są w absolutnej top lidze, jeżeli chodzi o zdolności do prowadzenia cyber, cyberoperacji. Najprawdopodobniej również o skutkach kinetycznych związanych na przykład z infrastrukturą krytyczną. To nie zostało uruchomione, oby nie zostało uruchomione. Ale z drugiej strony, no byłoby się głupim, gdyby się do takich scenariuszy nie przygotowywać.

Prowadzący: Słuchaj, na koniec chciałbym wrócić jeszcze do pewnych aspiracji haaktywistów, jeśli tak to mogę nazwać. Może nasi słuchacze również się spotkali z postami czy informacjami, nawołującymi w pewnym sensie do dołączenia do globalnych ataków na infrastrukturę IT Rosji. Trochę na zasadzie – zostań hakerem w naszej sprawie, jeżeli nim nie jesteś nauczymy cię lub chociaż wykorzystamy cię do ddsowania infrastruktury Rosji. Jak tego typu kampanie wychodzą? I jakie są płynące zagrożenia dla czasem nie do końca świadomych uczestników takich kampanii? Czyli takie prawdziwe oblicze pospolitego ruszenia.

Mirosław Maj: Cieszę się, że proponujesz ten temat, bo on jest bardzo ważny i może właśnie dotyczyć już, co chwilę już mówimy o instytucjach, organizacjach i poważnych sprawach, a przecież to jest, to jest sytuacja, w której każdy z nas gdzieś tam myśli, jak pomóc Ukrainie, prawda. I teraz, no każdy mówi, a to ja pomogę w tym, na czym się znam. I teraz może być taka pokusa, o której mówisz.

[01:00:00]

Mirosław Maj: Ja ze względów, no raz, że doktrynalnych, ale nawet jakbym je odłożył na bok, to bym powiedział w takich bardzo praktycznych, no to absolutnie bym nie doradzał takich, podejmowania takich działań. Wręcz bym nawoływał do tego, żeby ich absolutnie nie robić. Dlaczego? No myślę, że

jakby pierwsza przyczyna to jest taka, że one mimo tego, co my czytamy, obserwujemy, to one w rezultacie mają i tak dosyć ograniczone realny skutek. I żeby, gdyby ktoś chciał czysto utylitarnie podejść jakby do sprawy, nie wchodząc jakby w różne rozważania, powiedzmy, że odkładamy je na bok, dotyczące nie wiem, jakichś tam spraw związanych z tym, jak to powinno być poprawnie zorganizowane, kto to powinien robić, o czym za chwilę możemy jeszcze dwa słowa powiedzieć. Ale tak utylitarnie, czym my jesteśmy w stanie zaszkodzić? No jesteśmy w stanie, że tak powiem, taki, taki szum zrobić prawda, i trochę popsuć. Na pewno to gdzieś tam w swojej masie, w szczególności przy tym konflikcie tak, jak sobie mówiliśmy z dużym prawdopodobieństwem, no i jedna z największych, jeśli nie największa operacja anonimowych historycznie. Nie chcę powiedzieć, że to zupełnie nie ma znaczenia. No, bo jakby ktoś po drugiej stronie musi z tym walczyć, musi sprawdzać, musi się borykać z konsekwencjami wycieków pewnych danych i tak dalej. To takie pospolite ruszenie w sieci zawsze pewien skutek będzie miało. Ono nie będzie miało żadnego, że tak powiem, no przełomowego, tak. To po prostu, raczej to się tutaj nie, nie wydarzy. Natomiast jest związane co, jeżeli dobrze zinterpretowałem jakby Twoje pytanie to, co się w nim przewijało, to z pewnym ryzykiem, tak. To dzisiaj od takich prostych schematów, tak no rodem jeszcze z 2007 roku, czyli słynnego zaatakowania Estonii w sieci atakami ddos. No, które polegały również na tym, że no oddawało się kontrolę nad swoimi, nad swoimi komputerami po to, żeby ktoś mógł zarządzać tą siecią botnet. Dzisiaj to zjawisko, mimo że minęło 15 lat, to wcale nie zniknęło. No dzisiaj dużo ataków, no na przykład ddsowych oprócz tego, że jeszcze w między czasie powstały bardziej nowatorskie techniki, typu Amplification DDoS attack, no to nadal również jednak odbywają się w warstwie takiej klasycznej zarządzania sieciami botnetowymi. No i nie wiem, czy to jest dobry pomysł, żeby ze względu na nawet dobre, szczere intencje oddawać władanie swojego komputera komuś, kto jeszcze wczoraj był przestępcą. Dzisiaj mimo takich działań, no on gdzieś tam się nazywa jakimś ewentualnie aktywistą, tak, a pojutrze znowuż będzie przestępcą i będzie musiał odrabiać straty finansowe związane z tym, że właśnie był na wojnie i nie mógł zarabiać. To, o czym sobie mówiliśmy prawda, przed chwilą i mówię, teraz ten botnet może być zupełnie w inny sposób wykorzystany. Więc to, to są, to jest ryzyko. Najróżniejsze to zarówno tego, że jakby tracimy w niektórych przypadkach uczestnictwa tego kontroli nad swoimi komputerami, narażamy się na ataki, na ataki innych. No przecież druga strona nie siedzi po prostu w pieleszach i nie popija sobie ciepłej herbaty, obserwując to, tylko na przykład zbiera dane na temat tego, kto w tych atakach uczestniczy i być może, jeżeli będzie miała potrzebę sparaliżowania albo, albo zlikwidowania takich, takich botnetów, no to staniemy się ofiarami takiego ataku. A ci, którzy nas namawiają do niego, do przystąpienia, no to rzadko, kiedy, ja bym powiedział, że ja właściwie w ogóle się nie spotkałem z taką informacją, no mówili o takich ryzykach, czy mówili na przykład, jak zabezpieczyć swój komputer

w związku z tym, że idziesz na, idziesz na wojnę, tak. Czyli nikt ci nie rozdaje kamizelki kuloodpornej, tylko mówi po prostu – weź tutaj rozepnij koszulę i z okrzykiem hura na ustach, po prostu atakuj. To jest wszystko dosyć niebezpieczne. Do niczego to dokładnie nie prowadzi. Co więcej, ja miałem swego czasu okazję rozmawiać z ludźmi z Ukrainy, którzy w 2014 roku koordynowali działania ukraińskie, jeżeli chodzi o odpieranie ataków, o tą całą działalność w cyberprzestrzeni, na froncie przecież też z Rosją. I mówili, jak ich pytałem o to, co było ich, jakie były największe problemy, no to jednym z nich, które wymienili to jest, to była działalność zupełnie nieskoordynowanych grup haktywistów, aktywistów sieciowych, nad którymi oni nie mieli żadnego panowania. I mimo tego, że podejmowali oni jakieś próby rozmawiania i skoordynowania tej działalności, nawet według tej naszej opowieści uważając, że być może jakiś cel pozytywny jest do osiągnięcia, no to było zupełnie niekontrolowane.

[01:05:10]

Mirosław Maj: Co prowadziło de fakto do tego, że oni mieli czasami jeszcze więcej problemów, ponieważ ich szykowane operacje obronne, czy powiedzmy zaczepne, no mogły być w sprzeczności z tym, co obserwowali, tak. Co się działo, jeśli chodzi o to działanie, no grup, które, no właściwie no były sprzymierzeńcami tak, formalnymi takimi tak, z punktu widzenia, patrząc na to z lotu ptaka, byli sprzymierzeńcami. No, a w praktyce, jeśli chodzi o poszczególne operacje wcale to nie pomagało, nieraz bardzo, bardzo utrudniało. I to pokazuje, jak w ogóle działalność znowuż może niektórzy zrozumieli to odwołując się do zjawisk, które dzisiaj obserwujemy na przykład na dworcach kolejowych, gdzie próbujemy pomóc Ukraińcom. To nie jest tak, że jeżeli my pojawimy się kolejną grupką po prostu, która chce pomóc, to my dużo poprawimy. Może coś poprawimy, bo parę kanapek rozdamy i komuś coś podpowiemy, a może ktoś zabierze kogoś do domu. Natomiast to jest zupełnie inaczej, w momencie, kiedy takie, taka działalność by była skoordynowana i ktoś potrafiłby zarządzić tymi, tymi zasobami. To dokładnie jest tak samo, jeżeli chodzi o cyberprzestrzeń i włączanie się w tego typu działalność. Także, no podsumowując tą dłuższą wypowiedź – nie, nie, po prostu, to nie jest sposób na uczestnictwo w konflikcie w cyberprzestrzeni.

Prowadzący: Mirku, bardzo Ci dziękuję za dzisiejszą rozmowę i masę informacji, które dzisiaj poruszyłeś.

Mirosław Maj: Serdecznie dziękuję. Cieszę się, że podjąłeś ten temat. Jest dzisiaj już sporo doświadczeń z tego, co przy okazji wojny na Ukrainie się dzieje, powinniśmy o tym rozmawiać, na szybko wyciągać wnioski i podejmować już pewne, pewne akcje, a na pewno wynosić duże doświadczenia i od poziomu jakby poszczególnych internautów, do poziomu koordynacji krajowego systemu cyberbezpieczeństwa poprawiać każdy z tych elementów.

Prowadzący: Dzięki wielkie. Do usłyszenia w kolejnym odcinku.

Mirosław Maj: Dziękuję serdecznie.