aut. Paweł Ziemnicki 20.02.2019

FUNDAMENTALNE ZNACZENIE ZABEZPIECZENIA SATELITÓW PRZED CYBERATAKAMI [WYWIAD]

„Wdrażana przez ICEYE technologia zobrazowania powierzchni Ziemi z wykorzystaniem radarów SAR na mikrosatelitach może skupiać zainteresowanie sił zbrojnych. Ponadto wykorzystaniem tego typu systemów mogą być zainteresowani klienci, dla których kluczową sprawą jest poufność informacji. Stąd w działaniach przedsiębiorstwa należało zadbać o szeroko pojęte bezpieczeństwo" – tłumaczy Krzysztof Węgrzynek, odpowiedzialny za cyberbezpieczeństwo w firmie ICEYE.

Paweł Ziemnicki: Na czym polega Twoja praca dla ICEYE?

Krzysztof Węgrzynek: To długa historia. Mówiąc w skrócie, po skończeniu studiów nie do końca wiedziałem, czym chcę się zajmować. Wkrótce czymś takim, szczególnie interesującym dla mnie, okazało się bezpieczeństwo – szczególnie takie zagadnienia jak włamywanie się do systemów czy zabezpieczanie banków. Udało mi się w ten sektor wejść.

Czyli chodzi konkretnie o cyberbezpieczeństwo?

Tak, cybersecurity. W tym sektorze pracowałem przez dwa lata w Warszawie, zabezpieczając różne banki polskie i zagraniczne. Następnie wyjechałem do Londynu i później nieco podróżowałem po świecie. Udało mi się dzięki temu poznać światowe trendy w zakresie bezpieczeństwa cybernetycznego.

Wkrótce okazało się, że dynamicznie rozwija się firma ICEYE. Już wcześniej znałem jednego z jej założycieli – Rafała Modrzewskiego. Kilkakrotnie miałem też okazję odwiedzić Finlandię.

Czytaj też: Szybciej, taniej, we współpracy. New Space w wydaniu ICEYE [RELACJA]

Wdrażana przez ICEYE technologia zobrazowania powierzchni Ziemi z wykorzystaniem radarów SAR na mikrosatelitach może skupiać zainteresowanie sił zbrojnych. Ponadto wykorzystaniem tego typu systemów mogą być zainteresowani klienci, dla których kluczową sprawą jest poufność informacji. Stąd w działaniach przedsiębiorstwa należało zadbać o szeroko pojęte bezpieczeństwo. Chodzi o bezpieczeństwo samych satelitów, systemów komunikacyjnych, a także naziemnych systemów komputerowych, które są tu użytkowane podobnie jak w wielu innych firmach.

Praca przy zabezpieczeniu infrastruktury informatycznej ICEYE, jest ciekawa, bo mamy do czynienia z satelitami, systemami operacyjnymi oraz różnymi systemami komunikacyjnymi. Nie ma tu nudy, a fakt, że działamy w segmencie kosmicznym, stanowi dla mnie dużą wartość dodaną.

Jak zaczęła się Twoja przygoda z obecnym stanowiskiem pracy?

Po to, by zajmować się bezpieczeństwem, trzeba od podstaw zrozumieć działanie wykorzystywanych w przedsiębiorstwie systemów. Musiałem poznać wszystkie systemy od zera i przeprowadzić rozmowy z wieloma osobami, by dowiedzieć się jak to wszystko działa.

Zdobyta wiedza przydała mi się, a koledzy z firmy zaproponowali, że obok satelitów mógłbym nadzorować również działanie systemów naziemnych. Odpowiadam także za firmowe systemy IT. Pełnię obecnie niejako trzy funkcje naraz. W pewnym momencie zapewne będzie trzeba jakoś tę odpowiedzialność rozdzielić.

Czy samo przesyłanie danych z satelitów na Ziemię jest szyfrowane i zabezpieczone?

Tak, jak najbardziej. To jeden z elementów, których istotę dostrzegliśmy już na samym początku. Jako, że taki satelita krąży wokół Ziemi, to można w zasadzie próbować nawiązać z nim połączenie z dowolnego miejsca na planecie – na przykład z Chin. Satelita przelatuje nad tym regionem, więc różne jednostki mogą próbować się z nim połączyć lub podsłuchiwać, co jest przesyłane w ramach komunikacji z satelitą. Jeżeli ta komunikacja nie byłaby szyfrowana, wówczas byłoby niezwykle prosto ją podsłuchać.

W związku z powyższym, oba nasze kanały komunikacji – ten do zarządzania pracą satelity i drugi, służący do ściągania danych – wykorzystują techniki kryptograficzne. Są to standardowe mechanizmy używane w internecie. Jest to dobrze zabezpieczone. Był to jeden z tych projektów, które wdrażaliśmy przed wystrzeleniem pierwszego satelity.

Jak wyglądają obecnie światowe trendy, jeśli chodzi o cyberbezpieczeństwo satelitów?

Kiedy zaczynałem pracę w ICEYE, umiarkowanie interesowała mnie ta część związana z zabezpieczeniem systemów komputerowych w firmie. To bowiem wygląda tu mniej więcej tak samo, jak w każdym innym przedsiębiorstwie.

Bardzo interesowały mnie systemy związane z komunikacją z satelitą i działanie samego satelity. Jest taka jedna konferencja na świecie – CyberSat Summit w USA – która zbiera osoby z sektora bezpieczeństwa satelitarnego w jednym miejscu. Uczestniczyłem w niej. Niezwykle ciekawym doświadczeniem była dla mnie możliwość poznania dedykowanych tym zagadnieniom firm, szczególnie tych amerykańskich, które są bardzo zamknięte na rynek europejski. Kwestie bezpieczeństwa są przez regulacje eksportowe bardzo ściśle kontrolowane, stąd część rozwiązań nie wychodzi poza granice USA.

Zetknąłem się także z kilkoma firmami z Wielkiej Brytanii, które zajmują się bezpieczeństwem satelitów. Z rozmów z tamtejszymi specjalistami wynikło, że jest sporo potencjalnych zagrożeń dla satelitów, którym warto przyjrzeć się bliżej.

Czytaj też: ICEYE dąży do stworzenia centrum R&D w Krakowie [WYWIAD]

Co to za zagrożenia?

Przykładowo, można próbować tak zmieniać sygnał, który jest wysyłany do odbiornika radiowego satelity, wykorzystując potencjalne błędy w tym odbiorniku, żeby sygnał spowodował zdalne wykonanie kodu. W ten sposób można nawiązać nieautoryzowaną komunikację i spowodować wykonanie przez instrumenty satelity polecenia na podstawie nieautoryzowanego kodu. Tego rodzaju atak można eskalować na dalsze systemy. Byłby to jeden z takich ataków, które są trudne do wykrycia, ale i do przeprowadzenia. Tym niemniej, słyszałem, że jednej firmie z USA udało się coś

takiego przeprowadzić.

Usługi związane z bezpieczeństwem cybernetycznym rozwijają się bardzo mocno. Ma to zastosowanie w technologiach bezprzewodowych takich jak WiFi, Bluetooth czy RFID. Natomiast firmy świadczące tego typu usługi nie mają praktycznie dostępu do platform satelitarnych, przez co nie są w stanie zbudować kompetencji w tym zakresie.

Ostatnio byliśmy w kontakcie z organizatorami konferencji DEF CON, którzy podobno chcą podczas tej konferencji uruchomić Satellite Hacking Village. Rozmawialiśmy o tym, że być może coś uda się zrobić wspólnie.

Widzicie potencjał na współpracę z innymi przedsiębiorstwami na tym polu?

Jeśli jakaś inna firma dowie się, że robimy takie rzeczy i stwierdzi, że też chce się zająć tym tematem, to my jesteśmy bardzo otwarci na współpracę. ICEYE kojarzony jest z produkcją satelitów SAR, a informacje o tym, że chcemy być w czołówce jeśli chodzi o zabezpieczanie tak satelitów, jak i systemów naziemnych, nie są jeszcze dobrze rozpowszechnione.

Krzysztof Węgrzynek *– inżynier telekomunikacji, mocno związany z sektorem cyberbezpieczeństwa. Brał udział w zabezpieczaniu światowych banków w Polsce i za granicą Został wielokrotnie wyróżniony przez wiodących dostawców takich jak Microsoft, Cisco czy Sony za pomoc w zabezpieczaniu ich rozwiązań. Wcześniej pracował nad systemami komunikacyjnymi opartymi o satelity w brytyjskim Surrey Space Centre, przy Uniwersytecie Surrey. Prowadzi zespoły IT, bezpieczeństwa i infrastruktury naziemnej w ICEYE.*

Artykuł powstał przy współpracy z ICEYE.