http://poznan.wyborcza.pl/poznan/7,105531,23029225,cellary-wojna-w-sieci.html

Wojciech Cellary 2018-02-16

Cyberbezpieczeństwo

W pierwszych dniach stycznia tego roku byłem na konferencji ICCS (International Conference on Cyber Security) na samym środku Manhattanu w Nowym Jorku, tuż obok sławnej Metropolitan Opera. Nie byłoby w tym może nic nadzwyczajnego, bo często uczestniczę w konferencjach, ale ta konferencja była szczególna. Zorganizowało ją bowiem FBI wspólnie z Fordham University. O jej randze świadczy najlepiej to, że pierwszego dnia otwierający wykład miał urzędujący dyrektor FBI Christopher A. Wray, drugiego dnia – były szef CIA John O. Brennan, a trzeciego dnia – specjalny asystent prezydenta USA i koordynator ds. cyberbezpieczeństwa w Białym Domu Rob Joyce. W konferencji wzięło udział 350 uczestników z 48 krajów. Na sali były osoby reprezentujące bardzo różne zawody: naukowcy, informatycy, politycy, prawnicy, wojskowi w randze generała, agenci służb specjalnych i policji oraz przedstawiciele różnych biznesów – od takich, które prowadzą biznes przez internet na skalę globalną, po wyspecjalizowane w zabezpieczeniach przed cyberatakami. Duża część konferencji była zorganizowana w formie paneli dyskusyjnych, co bardzo angażowało uczestników. Ja występowałem w panelu poświęconym problemom międzynarodowym cyberbezpieczeństwa i prezentowałem europejski punkt widzenia na ochronę prywatności. Ta tematyka jest bardzo na czasie w związku w wejściem w życie w maju tego roku w całej Unii Europejskiej Rozporządzenia Ogólnego o Ochronie Danych Osobowych, czyli RODO, które zasadniczo zmienia reguły gry w zakresie ochrony prywatności zwiększając odpowiedzialność przedsiębiorstw i to nie tylko europejskich, ale wszystkich operujących na wspólnym rynku.

Z perspektywy takiej konferencji, jak ICCS, widać, jak bardzo świat się zmienił, i jak bardzo stanowi system naczyń połączonych. Internet spowodował, że koncepcja suwerennego państwa z jasno wytyczonymi granicami bronionymi przez żołnierzy uzbrojonych w karabiny nijak nie przystaje do współczesnych zagrożeń. Dzisiaj zagrożeniem jest atak przez internet przeprowadzony przez niewidocznego przeciwnika nie wiadomo skąd. Jeśli w wyniku takiego ataku zostaną wyłączone elektrownie, to bez jednego wystrzału cały kraj zostanie sparaliżowany. Skuteczny atak na system bankowy spowodowałby, że kraj zostałby pozbawiony pieniędzy, co unieruchomiłoby jego gospodarkę. W dodatku do przeprowadzenia takiego ataku na niedostatecznie zabezpieczony system nie potrzeba satelitów, rakiet, okrętów i łodzi podwodnych, na które stać tylko najbogatsze państwa, tylko laptop i wiedzę.

Na konferencji ICCS ciekawa była klasyfikacja hakerów i ich motywacji. Pierwszą grupę stanowią hakerzy, którzy włamują się dla pieniędzy. Albo kradną pieniądze z kont, albo numery kart płatniczych, by za ich pomocą ukraść pieniądze. Mogą wykradać tajemnice przemysłowe dotyczące nowoczesnych technologii, albo tajemnice, których znajomość pozwala przewidzieć

zmiany wyceny akcji spółek na giełdach, na czym można się wzbogacić. Mogą wykradać adresy mejlowe, aby sprzedać je spamerom. Mogą zaszyfrować czyjś komputer, by żądać zapłaty za odszyfrowanie. Mogą wreszcie szantażować ludzi, których okradli z tajemnic.

Drugą grupę stanowią haktywiści, czyli hakerzy walczący o jakąś sprawę, ideę, w którą wierzą. Włamują się, co jest nielegalne, aby zwrócić uwagę na tę sprawę lub aby upublicznić nadużycia i nieprawidłowości, które wymykają się systemowi sprawiedliwości.

Wreszcie trzecią grupę stanowią hakerzy motywowani politycznie, działających z ramienia politycznego mocodawcy, często obcego państwa. Są oni wspomagani przez internetowych trolli, którzy działają w mediach społecznościowych. Ich wspólnym zadaniem jest otumanienie demokratycznego społeczeństwa tak, aby w wyborach większość zagłosowała zgodnie z wolą ich politycznego mocodawcy.

Świat się zmienił. Bez internetu nie da się żyć, tak jak nie da się żyć bez elektryczności, czy bez pieniędzy. Wiemy, że elektrownia może wybuchnąć, a pieniądze może pożreć inflacja i od dawna bardzo się przez tym zabezpieczamy. Jednak wyzwaniem współczesności jest zabezpieczenie internetu. To jest zadanie dla wszystkich – do wojska i służb specjalnych, przez przedsiębiorstwa i instytucje publiczne, po każdego indywidualnego internautę. O bezpieczeństwie wszystkich decyduje bowiem najsłabsze ogniwo.