OPINIA WIIS nr 2/2018

Autor: Karol Cheda

WARSZAWSKI INSTYTUT
INICJATYW STRATEGICZNYCH

ROSYJSKA FALA CYBRATAKÓW

16 kwietnia br. amerykański i brytyjski rząd wystosowały ostrzeżenie przed mającą miejsce w cyberprzestrzeni „szeroką kampanią wymierzoną w routery i firewalle". Ataki przekroczyły liczbę miliona dotkniętych urządzeń na całym globie, godząc nie tylko w administrację rządową, ale również w firmy sektora prywatnego, organizacje utrzymujące infrastrukturę krytyczną oraz dostawców usług internetowych zapewniających wsparcie i prawidłowe działanie obu sektorów. **Przeprowadzona operacja miała służyć celom szpiegowskim, transferowi rozwiązań technologicznych, a także tworzyć w systemach bezpieczeństwa „tylne wejście" ułatwiające dalszą penetrację.** Pomimo braku jednoznacznych dowodów, specjaliści z Departamentu Bezpieczeństwa Krajowego USA wskazują na Federację Rosyjską jako sprawcę tych incydentów.

Wyżej wymienione ataki mogą stanowić część szerokiej kampanii działań w cyberprzestrzeni jaką Federacja Rosyjska prowadzi począwszy od szeroko znanych ataków w Estonii z maja 2007 roku. Jej natężenie uległo zwiększeniu w ostatnich latach, kiedy zdolność do prowadzenia działań w cyberprzestrzeni została oficjalnie uznana za priorytetową, co znalazło odbicie w deklaracji podsumowującej szczyt NATO w Newport. **Doskonałym poligonem doświadczalnym dla jej rozwoju stała się objęta konfliktem Ukraina, gdzie m.in. zastosowano oprogramowanie NotPetya, którego działanie polegało na szyfrowaniu danych, przede wszystkim tych kluczowych dla funkcjonowania infrastruktury państwowej oraz sektora prywatnego, a następnie ich uszkadzaniu, tak aby nie były możliwe do dalszego użytkowania.** Te działania mogły być testem zdolności paraliżu państwa za pomocą środków cybernetycznych.

Przypadek ten może również świadczyć o strukturalnej przemianie charakteru działań w cyberprzestrzeni – **znaczenie zorganizowanych grup hackerskich finansowanych przez państwo, które dostarcza im całą infrastrukturę wraz z najnowszymi rozwiązaniami technologicznymi ulega stałemu wzrostowi.** W związku z wciąż rosnącą profesjonalizacją działań w cyberprzestrzeni, konieczna jest intensyfikacja starań prowadzących do zmiany świadomościowej dotyczącej ewolucji form prowadzenia operacji militarnych, której pełnoprawnym elementem stała się wojna w cyberprzestrzeni i co za tym idzie, pole walki zaczęło przybierać nowe oblicze, charakteryzujące się pomimo braku formalnego stanu wojny pomiędzy rywalizującymi państwami zauważalną ciągłością.

OPINIA WIIS nr 2/2018

Autor: Karol Cheda

WARSZAWSKI INSTYTUT INICJATYW STRATEGICZNYCH

POLSKI PUNKT WIDZENIA:

Polska, graniczący z Federacją Rosyjską, znajduje się w jej najbliższym obszarze operacyjnym. W związku z rosyjską polityką dążenia do rekonstrukcji porządku zimnowojennego poprzez znaczne rozszerzenie strefy wpływów, **jest w pierwszym rzędzie państw narażonych na cyberataki. W tym kontekście szczególnej uwagi wymagają przewidziane na jesień br. wybory samorządowe.**

Priorytetową kwestią wydaje się zatem być **jak najszybszy rozwój zdolności do prowadzenia działań w cyberprzestrzeni.** Kluczowymi czynnikami dla stworzenia systemu cyberobrony RP są:

- utworzenie spójnej strategii operacyjnej;

- konstrukcja systemu CSiRT-ów (Computer Security Incident Response Team);

- budowa systemu szkolenia specjalistów;

- ale także często lekceważone propagowanie dobrych praktyk;

Fala rosyjskich ataków obierała na cel podstawowe urządzenia składowe sieci teleinformatycznych takie jak routery, infekując te, które były niedostatecznie zabezpieczone. **Szczelność systemu cyberbezpieczeństwa zależy od jego najgorzej chronionego elementu, dlatego nawet najnowsze rozwiązania technologiczno-instytucjonalne nie zapewnią odpowiedniego poziomu zabezpieczeń jeśli zawodny okaże się nieodpowiednio przeszkolony czynnik ludzki.**

Na podstawie:

- B. Jansen, E. Weise, *Russia is sponsoring cyberattacks in U.S. homes and businesses, U.S. and U.K. officials warn*, USA Today, https://www.usatoday.com/story/news/2018/04/16/russia-sponsoring-cyberattacks-u-s-homes-and-businesses-u-s-and-u-k-officials-warn/520981002/

- N. Lomas, *UK accuses Russia of 2017's NotPetya ransomware attacks*, Tech Crunch https://techcrunch.com/2018/02/15/uk-accuses-russia-of-2017s-notpetya-ransomware-attacks/

- U.S. Department of Homeland Security, https://www.dhs.gov/

- Edict of the Russian Federation President on the Russian Federation's National Security Strategy, http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf