Na straży bezpieczeństwa cybernetycznego

Takie były początki (choć może niekoniecznie początki)

Prezydent Obama powołał 22 grudnia 2009 roku Howarda A. Schmidta na stanowisko koordynatora bezpieczeństwa cybernetycznego. Schmidt będzie koordynować działania agend rządowych w celu zabezpieczenia USA przed cyberatakami i wzmacniania bezpieczeństwa sieci komputerowych wspólnie z prywatnymi firmami odpowiedzialnymi za 80% kluczowych systemów.

Schmidt powiedział podczas uroczystości w Białym Domu, że nasz cyfrowy świat stwarza wiele możliwości, ale też wielkie zagrożenia. Jego zadaniem jest kontakt bezpośredni z prezydentem, odpowiedzialność przed Radą Bezpieczeństwa Narodowego i współpraca z Narodową Radą Gospodarczą w kwestiach cyberbezpieczeństwa.

Rządowe systemy komputerowe USA są atakowane miliony razy dziennie przez hakerów, którzy wykorzystują zaawansowane technologie do kradzieży informacji i środków finansowych. Wywiady obcych państw próbują uzyskać poufne dokumenty i technologie oraz uszkodzić sieci odpowiedzialne za dostarczanie usług.

Stanowisko koordynatora ds. cyberbezpieczeństwa zostało utworzone w maju 2009 po dwumiesięcznej ocenie sytuacji cyfrowego bezpieczeństwa USA. Pierwszym koordynatorem była Melissa Hathaway.

Jak zabezpieczone są inne państwa, jak sytuacja wygląda w innych państwach

Każde państwo ma własne strategie i narzędzia do zabezpieczania swoich sieci komputerowych i chronienia swoich

informacji i danych. Niektóre państwa, takie jak Stany Zjednoczone, mają specjalne agencje i stanowiska zajmujące się bezpieczeństwem cybernetycznym, podczas gdy inne państwa koncentrują się na innych aspektach ochrony swoich sieci. Stopień zabezpieczenia różni się w zależności od państwa i jest wynikiem wielu czynników, w tym budżetu i poziomu zaawansowania technologicznego.

W Polsce bezpieczeństwo cybernetyczne jest ważnym zadaniem rządu i jest regulowane przez kilka instytucji, w tym Ministerstwo Cyfryzacji oraz Inspekcję Ochrony Danych Osobowych. Polska armia również ma swoje jednostki zajmujące się bezpieczeństwem cybernetycznym. W Polsce istnieją również firmy prywatne i organizacje pozarządowe, które zajmują się zabezpieczaniem sieci i danych. Mimo to, Polska jak i wiele innych państw, nie jest wolna od cyberataków i nieustannie musi się dostosowywać i ulepszać swoje narzędzia ochrony, aby zabezpieczyć swoje systemy przed nowymi zagrożeniami.

Tylko nie wiadomo, czy rząd dba o bezpieczeństwo obywateli, czy może sam jest zagrożeniem.

Pegasus

Pegasus to narzędzie stworzone przez izraelską firmę NSO Group, służące do inwigilacji i przechwytywania danych z urządzeń mobilnych. Zostało ono ujawnione w 2019 roku i jest znane z tego, że było używane do śledzenia dziennikarzy, aktywistów i obrońców praw człowieka w różnych krajach na całym świecie. Pegasus wykorzystuje luki w oprogramowaniu systemów operacyjnych, takich jak iOS i Android, aby uzyskać dostęp do danych urządzenia.

Jeśli szukają Państwo pomocy w napisaniu własnej pracy - potrzebują Państwo fachowych konsultacji to polecamy stronę pisanie prac - profesjonalna pomoc w pisaniu prac w granicach prawa.