Uważaj. Wirusy potrafią się chować nawet ponad 200 dni

Kategoria: Styl życia
Opublikowano: wtorek, 17, październik 2017 11:27
Artur Duda

Codziennie dochodzi do tysięcy ataków hakerskich. Tylko między 2015, a 2016 rokiem ich liczba wzrosła o ok. 300 proc., pokazują dane Komisji Europejskiej. Zagrożeń jest nie tylko więcej, są także coraz bardziej zaawansowane, a przez to groźniejsze do wykrycia i zneutralizowania. Nawet przez ponad 200 dni możemy nie wiedzieć o infekcji systemu.

- *Ataki stają się coraz bardziej perfidne i przed tym nie ma ucieczki. Dane statystyczne pokazują, że średni czas od momentu infekcji do wykrycia specjalnie napisanego pod daną firmę wirusa wynosi około 201 dni. Wirus Carbanak działał 2 lata. W tym czasie zainfekował ponad 100 banków, którym skradziono ponad miliard dolarów. Infekcję wykryto przypadkiem* - mówi newsrm.tv Paweł Franka, CEO VT Cyber i dodaje - *Malware często długo są cicho i mutują. Wirus zbiera dane i tak na prawdę nie wiemy co robią, bo systemy ich nie wykrywają.*

Innym typem zagrożenia są ataki ransomware. W ich przypadku od razu wiemy, że coś niedobrego się dzieje, gdyż tracimy dostęp do naszych danych. Przykładem takiego ataku był wirus Petya, który sparaliżował ukraińskie instytucje i spowodował ogromne straty finansowe firm. W wyniku ataku 300 mln dolarów stracił największy na świecie operator morskich transportów kontenerowych, duńska spółka Maersk.

- *Wiele furtek, przez które dochodzi do ataków są bardzo oczywiste. Często dostajemy jakiegoś maila z linkiem np. od nigeryjskiej księżniczki, która napisała „wyślij mi pieniądze, a ja Ci wyślę 20 milionów dolarów". O dziwo są osoby, które dają się na to złapać* - opowiada Piotr Oleszkiewicz, ekspert ds. cyberbezpieczeństwa.

Kolejną drogą, już mniej oczywistą, którą wykorzystują cyberprzestępcy jest połączenie systemów nowoczesnych i systemów, które istnieją od lat 20, 30. Atak może np. nastąpić gdy skanuje się plik tekstowy. - Stary tekstowy system nie rozpoznaje tego jako atak, bo jest to dla niego po prostu zwykły blok tekstu. Nowy system internetowy pobiera dane np. z systemu bankowego z pełnym zaufaniem nie weryfikując ich. W ten sposób, w przeglądarce klienta atak jest wykonany i traci on pieniądze - wyjaśnia Piotr Oleszkiewicz.

Atak hakerski może przeprowadzić praktycznie każdy. Nie trzeba mieć wiedzy programistycznej – obecnie cyberprzestępcę można po prostu wynająć. Wystarczy niewielka kwota, by dostać naładowaną broń. Skoro nawet międzynarodowi giganci nie są w stanie poradzić sobie z hakerami, czy polskie firmy mogą ochronić się przed cyberatakami?

- *Takich systemów które dają nam 100 procentową gwarancję nie ma jeżeli chcemy mieć połączenie z Internetem. Możemy minimalizować skutki ataków wykrytych, wykrywać je jak najszybciej, reagować jak najszybciej, skracać ten czas potrzebny do przywrócenia poprzedniego poziomu. Ataków nie unikniemy, zawsze będzie to wyścig z czasem* - dodaje Paweł Franka.

Cyberprzestrzeń jest wygodna i potrafi uśpić czujność. Dlatego potrzebne jest zabezpieczenie z wielu stron. Duże wycieki danych nie dzieją się przypadkiem i często poprzedza je aktywność, którą można wykryć poprzez analizę zachowania użytkowników. Nowym podejściem na świecie jest UEBA (User Experience Behavioral Analytics), które służy do obrony przed przypadkami długofalowego sabotażu, wykrywając nietypowe zachowania pracowników. Warto o tym pamiętać, bo niedługo za wyciek danych z baz firmom mogą grozić potężne kary finansowe.

Kategoria: Styl życia
Opublikowano: wtorek, 17, październik 2017 11:27
Artur Duda
Odsłony: 1781

- Zarządy firm przywiązują coraz większą wagę do cyberobrony przed atakami na infrastrukturę przemysłową, a także wymogów unijnego rozporządzenia dotyczącego ochrony danych osobowych (RODO). I słusznie, bo zagrożenie jest realne i może narazić całą spółkę na ogromne straty – wyjaśnia Paweł Franka. Dotyczy to zarówno wielkich korporacji, jak i małych firm. Hakerzy cały czas są o krok przed specjalistami od cyberbezpieczeństwa. Czy jest szansa na zmianę tej sytuacji?

- Brakującym ogniwem jest człowiek, który rozumie zarówno biznes, jak i sposób myślenia, a także metody działania cyberprzestępców - powiedział Piotr Oleszkiewicz.

Wypowiedź: Paweł Franka, CEO VT Cyber sp. z o.o., Piotr Oleszkiewicz, ekspert ds. cyberbezpieczeństwa.

Źródło: Newsrm.tv