NC Cyber: notujemy stały wzrost liczby incydentów w sieci

Od stycznia do października 2017 r. zespół CERT Polska, należący do działającego w NASK NC Cyber, obsłużył 647 incydentów związanych z malware, czyli złośliwym oprogramowaniem.

W całym 2016 r. takich incydentów było 211. Teraz komunikaty ostrzegawcze NC Cyber dostępne są już w RSO.

Łącznie wszystkich zgłoszeń do NC Cyber było w bieżącym roku pond 9 tys. W okresie od stycznia do końca października 2017 zespół CERT Polska w NC Cyber odnotował wśród tych zgłoszeń 221 prób włamań do zasobów informatycznych. To dwa razy więcej niż przez cały 2016 r., kiedy obsłużono 109 takich incydentów. Wzrost liczby obsłużonych przez CERT Polska incydentów nie oznacza bezpośrednio wzrostu liczby przestępstw komputerowych.

> *Wzrost wynika w naszej opinii przede wszystkim z rosnącej świadomości internautów. Coraz więcej osób zdaje sobie sprawę, jak ważne jest zgłaszanie wszystkich niepokojących zdarzeń do CERT Polska. To daje ekspertom możliwość analizowania nowego zagrożenia, szybkiej oceny, na ile jest poważne i dzięki temu ostrzegania kolejnych osób oraz instytucji zanim padną ofiarą przestępców* - komentuje dyrektor NC Cyber w NASK Juliusz Brzostek.

Jak dodaje, im więcej danych o konkretnym zagrożeniu zyskają specjaliści z NC Cyber, tym większa szansa, że wypracują metodę przeciwdziałania.
Właśnie w ten sposób powstają np. narzędzia do odblokowywania danych na komputerach zainfekowanych przez ransomware - oprogramowanie wykorzystywane przez szantażystów do szyfrowania danych ofiar w celu wyłudzenia okupu za ich przywrócenie. Ransomware jest jednym z najczęściej występujących niebezpiecznych

zjawisk w sieci. Aby wspomóc ofiary tego typu przestępstw, powstała globalna inicjatywa No More Ransom, w ramach której współdziałają najwyższej klasy specjaliści w dziedzinie cyberbezpieczeństwa z firm komercyjnych, instytucji publicznych (rządowych i pozarządowych) oraz ośrodków badawczych. "Do tej inicjatywy, która m.in. za darmo udostępnia narzędzia deszyfrujące, należy też CERT Polska" - przypomina szef NC Cyber.

Oddolne inicjatywy, angażujące do współpracy w wąskiej dziedzinie nie są jednak wystarczające, aby w zasadniczy sposób wpływać na krajobraz cyberbezpieczeństwa globalnie, jak i w poszczególnych krajach. Dlatego we wsparcie współpracy różnych podmiotów angażują się państwa i organizacje międzynarodowe, w tym Unia Europejska. Ministerstwo Cyfryzacji prowadzi konsultacje projektu ustawy o krajowym systemie cyberbezpieczeństwa, która ma dostosować prawo naszego kraju do wymogów dyrektywy Parlamentu Europejskiego i Rady w sprawie środków, mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (w skrócie NIS od angielskiego: *Network and Information Security*). Dyrektywa ma na celu budowę systemu współpracy w obszarze cyberbezpieczeństwa na poziomie państw członkowskich i w obrębie całej wspólnoty. Projekt ustawy o krajowym systemie cyberbezpieczeństwa zakłada przede wszystkim raportowanie przez wyznaczone, kluczowe firmy i instytucje incydentów zagrażających bezpieczeństwu w sieci do wyznaczonego centrum koordynacyjnego, które będzie odpowiedzialne za ocenę stopnia zagrożenia i wdrożenie dalszych działań oraz za prowadzenie współpracy międzynarodowej.

W myśl projektu ustawy, krajowy system cyberbezpieczeństwa obejmuje: operatorów usług kluczowych i dostawców usług cyfrowych, CSIRT (Computer Security Incident Response Team) MON, CSIRT NASK, CSIRT GOV, przedsiębiorców telekomunikacyjnych, organy publiczne oraz jednostki je obsługujące, sądy i trybunały, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Rządowe Centrum Bezpieczeństwa, jednostki podległe i nadzorowane przez organy administracji rządowej, jednostki samorządu terytorialnego oraz ich związki i zrzeszenia, uczelnie publiczne, Polską Akademię Nauk, podmioty świadczące usługi z zakresu cyberbezpieczeństwa i organy właściwe do spraw cyberbezpieczeństwa.

Ministerstwo Cyfryzacji informuje, że zapewnienie wysokiego poziomu cyberbezpieczeństwa to jeden z jego priorytetów. Uzasadniając projekt ustawy, resort

wyjaśnia, że nowe przepisy mają gwarantować m.in. niezakłócone świadczenie usług kluczowych z punktu widzenia państwa i gospodarki (szpitale, dostawy wody pitnej, energetyka, bankowość) oraz usług cyfrowych poprzez osiągnięcie wysokiego poziomu bezpieczeństwa systemów informacyjnych służących do ich świadczenia.

Ustawa powołuje także organy właściwe ds. cyberbezpieczeństwa, odpowiedzialne za sprawowanie nadzoru wobec operatorów usług kluczowych i usług cyfrowych. Powołuje również pojedynczy punkt kontaktowy ds. cyberbezpieczeństwa, prowadzony przez ministra właściwego do spraw informatyzacji, odpowiedzialny za wymianę informacji związanych z cyberbezpieczeństwem na poziomie kraju oraz współpracę transgraniczną na poziomie Unii Europejskiej.

Konsultacje publiczne ustawy o krajowym systemie bezpieczeństwa