Cyberdefence 24

aut. Tomasz Fastyn 17.08.2016

RAPORT ENISA: ILOŚĆ CYBERATAKÓW WZRASTA, ALE REALNE KOSZTY NADAL SĄ NIEZNANE

Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) w raporcie opublikowanym na początku tego miesiąca zajęła się zbadaniem realnych kosztów ataków cybernetycznych na infrastrukturę biznesową oraz państwową. Problemem według europejskiej agencji ma być brak wypracowanych standardów podejścia do tematyki cyberbezpieczeństwa oraz kryteriów wykorzystywanych w analizach.

Według autorów raportu początkowy problem w przypadku zagrożeń oraz rozmiarów ataków jest brak wspólnego języka przy analizie źródeł ataku. Sektory szczególnie narażone na ataki, jakimi niewątpliwie mają być tzw. CIIs czyli Krytyczna Infrastruktura Informacyjna mają być tego szeregowym przykładem. Jak czytamy w raporcie – brak wspólnego podejścia oraz kryteriów przy analizach spowodował sytuację w której istnieje wiele raportów, które nie pokrywają się tematycznie, czasami tylko w niewielu punktach – czytamy w raporcie „The cost of incidents affecting CIIs". Ma to tworzyć według autorów sytuacje paradoksalną w której tworzone jest wiele raportów dotykających podobnych kwestii bezpieczeństwa, jednak zupełnie różnych pod względem określenia co było problemem np. wycieku danych. Według twórców raportu dr Dan Tofan, Theodoros Nikolakopoulos and Eleni Darra brak tych założeń standaryzujących pojęcia czy podejścia do samej tematyki, czy choćby informowania o samy fakcie ataku leży u podstaw problemu braku współpracy. Dochodzi według nich nawet do sytuacji, w których niektóre firmy dotknięte atakami nie są nawet ich świadome, więc nie wiedzą nawet, że wyniki ich firmy są skażone działaniami osób trzecich. Bez wspólnego podejścia ich zdaniem nie ma co nawet myśleć o wspólnej obronie. To szczególnie ważne słowa, ponieważ Polska, tak jak inne kraje Unii Europejskiej będzie musiała dostosować się w pełni do nowej dyrektywy NIS w roku 2018.

W raporcie także da się zauważyć pewną rozczarowanie twórców jeżeli chodzi o analizę ekonomiczną ataków na sektor CIIs, według nich bez odpowiedniej ilości danych trudno będzie określić jakie realne przełożenie na funkcjonowanie firmy mają ataki DDoS, a jaki wpływ może mieć np. błąd pracownika. Bez tego, przynajmniej według raportu trudno stworzyć jedną politykę bezpieczeństw, która pozwoli na ochronę firm oraz administracji państwowej przed przyszłymi reperkusjami ataku.

Najpopularniejszym rodzajem ataku występującym w sektorze prywatnym oraz administracyjnym opisanym w raporcie ma być atak DDoS, tuż za nimi zagrożeniem mają być osoby pracujące wewnątrz firmy lub organizacji. W przypadku kosztów do jakich udało się dotrzeć badaczom ENISA jest akurat odwrotnie, to ataki z wykorzystaniem osób wewnątrz struktur mają być bardziej kosztowne od DDoS. Zaskoczenia także nie ma jeżeli chodzi o najcenniejsze co posiadają obecnie firmy – dane, informację, wszelkiego rodzaju pliki. Wszystko co jest możliwe do wykradzenia przy pomocy ataku hakerskiego. Problemem mają być także mechanizmy określające realne szkody spowodowane przez atak, wyciek danych. Firmy według raportu mają mieć problem ze zmierzeniem jakie koszty są związane z przywróceniem firmy do działania sprzed ataku.

ENISA oprócz analizy problemu podała kilka porad, które mają pomóc w tworzeniu raportu dotykającego kwestie cyberbezpieczeństwa:

- ilość firm, które wzięły udział w badaniu (wielkość próbki)
- analiza danych geograficznych
- organizację, które stworzyły raport oraz ich potencjalne interesy wynikające z jego tworzenia
- metodologia użyta podczas przeprowadzania badań
- wpływ na cały sektor
- rodzaj zagrożeń i incydentów branych pod uwagę w badaniu

Czytaj też: Już w listopadzie największe zawody cybernetyczne na terenie Europy