# NC Cyber: coraz więcej cyberzagrożeń przez błędy w oprogramowaniu

## Już kilkaset luk i błędów w popularnych usługach oraz oprogramowaniu znaleźli specjaliści CERT Polska w NASK. Ich wykrycie i przekazanie informacji producentom oraz środowisku specjalistów ds. bezpieczeństwa pozwala uchronić miliony użytkowników przed zagrożeniem, wynikającym z tych błędów.

"Podatności, czyli błędy umożliwiające przeprowadzenie ataku, są w zapewnianiu bezpieczeństwa kluczowym zagadnieniem. Wiedza o tym, że w popularnym oprogramowaniu jest luka, z której producenci i użytkownicy nie zdają sobie sprawy, może być dla przestępców warta kolosalne pieniądze" -  mówi Juliusz Brzostek, dyrektor NC Cyber.

Dlatego nierzadko zdarza się, że organizacje przestępcze płacą za informacje o nowych podatnościach lub nawet zatrudniają etatowych analityków, którzy ich poszukują. I często znajdują, ponieważ nie ma stuprocentowo bezbłędnych usług i aplikacji.

> Producenci na bieżąco wypuszczają "łatki" i aktualizacje, pozwalające usunąć znane luki. Kluczowe jednak jest to, aby były rozpoznane, co pozwala wykryć je zanim uda się to przestępcom - wyjaśnia Juliusz Brzostek.

Dlatego analitycy bezpieczeństwa również aktywnie poszukują podatności. Takie działania regularnie prowadzi również zespół ekspercki CERT Polska, będący częścią NC Cyber, działającego w NASK. Od czasu uruchomienia NC Cyber, czyli od lipca 2016 r. udało im się zidentyfikować 379 podatności i błędów w przeanalizowanych 46 różnego typu rozwiązaniach. Producenci, powiadomieni o problemie, poprawili 334 z tych błędów.

Ponadto, eksperci CERT Polska zarejestrowali 104 ze znalezionych podatności w publicznym słowniku CVE (Common Vulnerabilities and Exposures - ang. Znane

Podatności i Zagrożenia). Jest to międzynarodowa baza danych o znalezionych lukach w dostępnym na rynku oprogramowaniu. Korzystają z niej specjaliści i firmy z branży cyberbezpieczeństwa, np. producenci programów antywirusowych.