TO PAŃSTWA NAPĘDZAJĄ CZARNY RYNEK EXPLOITÓW UŁATWIAJĄC CYBERATAKI

Rządy państw narodowych swoją polityką wobec podatności oprogramowania na cyberataki stymulują rozwój czarnego rynku exploitów, które umożliwiają przejmowanie kontroli nad systemami komputerowymi.

W niedawnym wydaniu telewizyjnego magazynu „Quarks and Caspers" pt. *Wojna cebernetyczna*, emitowanym w niemieckim Westdeutscher Rundfunk stwierdzono jednoznacznie: "To państwa napędzają czarny rynek *exploitów*". W roli eksperta wypowiadał się dyrektor firmy softScheck i orędownik całkowitego ujawniania (*full disclosure*) informacji o podatnościach na atak (*vulnerabilities*) prof. dr Hartmut Pohl. Jego zdaniem, rządy i państwa są współodpowiedzialne za rozkwit czarnego rynku *exploitów* poprzez promocję prawną tzw. odpowiedzialnego ujawnienia (*responsible disclosure*).

Skąd się bierze problem?

Wypowiedź prof. Pohla oznacza powrót do wcześniejszych dyskusji o właściwości postępowania w przypadku wykrycia podatności na atak (*vulnerabilities*) w systemie, aplikacji badź części infrastruktury sieci. Zgodnie z aksjomatem głoszacym, że nie ma systemów w 100 proc. bezpiecznych i pozbawionych błędów w kodach bądź furtek (*backdoor*) dostępu, wykrycie takich podatności to kwestia czasu.

Najważniejsze pytanie brzmi: kto pierwszy wykryje podatność na atak. Uogólniając, możliwości są dwie: albo jest to tzw. dobry hacker (*white hat*) albo zły hacker (*black hat*). W pierwszym przypadku dobry hacker informuje producenta oprogramowania lub właściciela infrastruktury o wykrytej podatności. W drugim przypadku zły hacker nie informuje producenta i jednocześnie tworzy *exploit* - program mający na celu wykorzystanie błędów w oprogramowaniu bądź luk bezpieczeństwa. Zły hacker może wykorzystać wiedzę o podatności i stworzony program dla własnych celów bądź podzielić się nim z zainteresowanymi nabywcami za odpowiednią gratyfikacją (najczęściej finansową).

Handel *exploitami* w środowisku *dark net* stanowi poważny problem. W momencie, gdy *exploit* pojawia się na czarnym rynku przed publikacją poprawki przez producenta, nadaje się mu miano *zero-day exploit*. Sprzedawców kuszą przede wszystkim rynkowe ceny informacji o podatności i gotowych *zero-day exploitów*, które oscylują w granicach 1 tys. euro w przypadku *exploitów* dla mało znanych aplikacji, od 1 tys. do100 tys. euro dla aplikacji biznesowych bądź popularnych wśród użytkowników czy milionów euro, gdy w grę wchodzą najpopularniejsze aplikacje i serwisy (Facebook, Microsoft etc.). Oczywiście ceny podawane są w wirtualnych walutach takich jak bitcoin i dopuszcza się opcję licytacji.

Kto kupuje exploity od złych hakerów

Odpowiedź na to pytanie znaleźć można w definicjii *aktora zagrożenia cybernetycznego* (*cyber threat*

actor). Obecnie wyróżnia się trzy podmioty (*aktorzy*) najaktywniejsze w działaniach cybernetycznych:

1. cyberprzestępcy – ich głównym celem jest korzyść materialna, np. kradzież aktywów z kont bankowych, nielegalne rejestracje towarów, fałszowanie dokomentów, pozwoleń, certyfikatów;
2. haktywiści – ich głównym celem nie są pieniądze, a raczej cele polityczno-społeczne, np. szantaże polityczne, ataki cybernetyczne na wrogie grupy ludzi, organizacje, cyberterroryzm;
3. rządy państw – ich głównym celem pozostaje osłabienie wrogiego państwa, kradzież własności intelektualnej (szczególnie w dziedzinie technologii, wojskowości i medycyny), dostęp do materiałów kompromitujących (*компромат)* wysokiej rangi urzędników innych państw.

W 2015 r. portal ControlRisks opublikował szacunkowy udział procentowy trzech wymienionych wyżej *aktorów* w atakach cybernetycznych. Wynosił on odpowiednio 46 proc. dla przestępców, 33 proc. dla haktywistów i 21 proc. dla rządów państw.

Wybór celu ataku za pomocą *exploita* zależy od *aktora*. Cyberprzestępcy pokuszą się o atak na przeciętnego obywatela, firmę, bank etc. Haktywiści zapewne zaatakują polityków, wojskowych, strategiczne obiekty, instrastrukturę energetyczną i transportową. Rządy państw z kolei nakierują ataki na terrorystów, grupy wrogie własnemu, inne państwa, własnych obywateli podejrzewanych o działalność antypaństwową bądź kryminalną.

Teoretycznie może zdarzyć się też tak, że sam producent gotowy będzie zapłacić za nabycie furtki do własnego systemu, aby nie stracić reputacji u klientów i załatać (*patch*) lukę odpowiednio szybko. Naturalnie producent nie jest *aktorem* zagrożenia cybernetycznego, przynajmniej w stopniu aktywnym, gdyż w jego interesie pozostaje zwalczanie ataków i zapobieganie im.

Co powinien zrobić dobry haker

Dobry haker jako przedstawiciel etycznie działającej społeczności w żaden sposób nie powinien zatajać i sprzedawać informacji dotyczącej podatności na ataki. Wszak głównym jego celem jest zwiększenie bezpieczeństwa w Sieci przez przekazanie newralgicznej informacji odpowiednim osobom, aby uniemożliwić złym hackerom wykorzystanie podatności w postaci *zero-day exploitów*.

Dyskusja podjęta na antenie WDR przez prof. Hartmuta Pohla odwołuje się zarówno kontrowersji, jakie wywołuje kwestia ujawnienia informacji o podatnościach. Rozróżniamy trzy podejścia do niej:

1. *full disclosure* – pełne ujawnienie polegające na podaniu przez dobrego hackera informacji o podatności do wiadomości publicznej w momencie jej wykrycia;
2. *responsible or coordinated disclosure* – odpowiedzialne ujawnienie, które polega na poinformowaniu w pierwszej kolejności producenta w celu umożliwienia mu wprowadzenia poprawek - dopiero po wprowadzeniu poprawek przez producenta ujawnia się publicznie informację o tym, że we wcześniejszym okresie istniała podatność;
3. *non-disclosure* – nieujawnienie podatności

Ostatni z wariantów będzie interesował przede wszystkich *aktorów* zagrożeń cybernetycznych i oficjalnie w żadnym kraju prawo nie będzie wzmiankowało istnienia takiej możliwości. Jakkolwiek paradoksalnie to zabrzmi, rządy państw oczekują informacji o podatnościach od osób trzecich, podczas gdy same nie są do zobowiązane do dzielenia się swą wiedzą z kimkolwiek.

Full disclosure interesuje przede wszystkim naukowców, profesjonalistów, administratorów systemów, baz danych itp. W przypadku podania do wiadomości publicznej informacji o podatności, są oni w stanie przygotować swoje systemy na ewentualne zagrożenie.

Co mówi prawo o exploitach

Reponsible disclosure interesuje z kolei producentów, którzy po pierwsze nie chcą stracić reputacji przez nagłaśnianie podatności, a po drugie obawiają się, że w wyniku ujawnienia informacji niektórzy hackerzy podejmą się próby wykorzystania podatności. Obok producentów takie rozwiązanie promują oficjalnie także rządy państw i ich prawodawstwo. Kary za nielegalne wtargnięcie do systemu i przymus kontaktu z producentem są elementami porządku prawnego.

Rzymska maksyma *Dura lex, sed lex* z pewnością nie odnosi sie do prawa w zakresie teleinformatyki w poszczególnych państwach (np. Niemcy) czy ich konfederacjach (np. Unia Europejska). Obecne regulacje prawne obowiązujące w Republice Federalnej Niemiec i UE nie zawsze pozwalają na skuteczne rozwiązanie problemu handlu *exploitami*.

W budapeszteńskiej konwencji Rady Europy z 2001 r. dotyczącej cyberprzestępczości (*Convention on Cybercrime*) punkt 6 precyzuje *Nieprawidłowe użycie urządzeń (Misuse of devices*), zobowiązując wszystkie państwa członkowskie do wprowadzenia kar w przypadku wytwarzania, zaopatrywania, importu, dystrybucji i rozpowszechniania w jakikolwiek inny sposób:

a) urządzeń i komputerów, zaprojektowanych w celu nielegalnego dostępu lub intereferencji z danymi lub systemem;

b) haseł do komputerów, kodów dostępu lub jakiejkolwiek innej informacji dzięki której możliwy jest dostęp do części lub całości systemu komputerowego.

Z kolei *Decyzja ramowa (Framework Decision) 2005/222/JHA Rady UE* dotycząca ataków przeciwko systemom informatycznych, zobowiązuje wszystkie państwa członkowskie do wprowadzenie kar pozbawienia wolności za cztery rodzaje działaności:

a) nielegalny dostęp do systemu informatycznego (*illegal access to information systems*)

b) nielegalna ingerencja w system (*illegal system interference*)

c) nielegalna ingerencja w dane (*illegal data interference*)

d) nakłanianie do przestępstwa i pomoc w przestępstwie (instigation, aiding and abetting and attempt)

Minimalna kara pozbawienia wolności wynosi od 1 roku do 3 lat za bliżej niesprecyzowane „ przypadki, które nie są niewielkie” (for cases which are not minor).

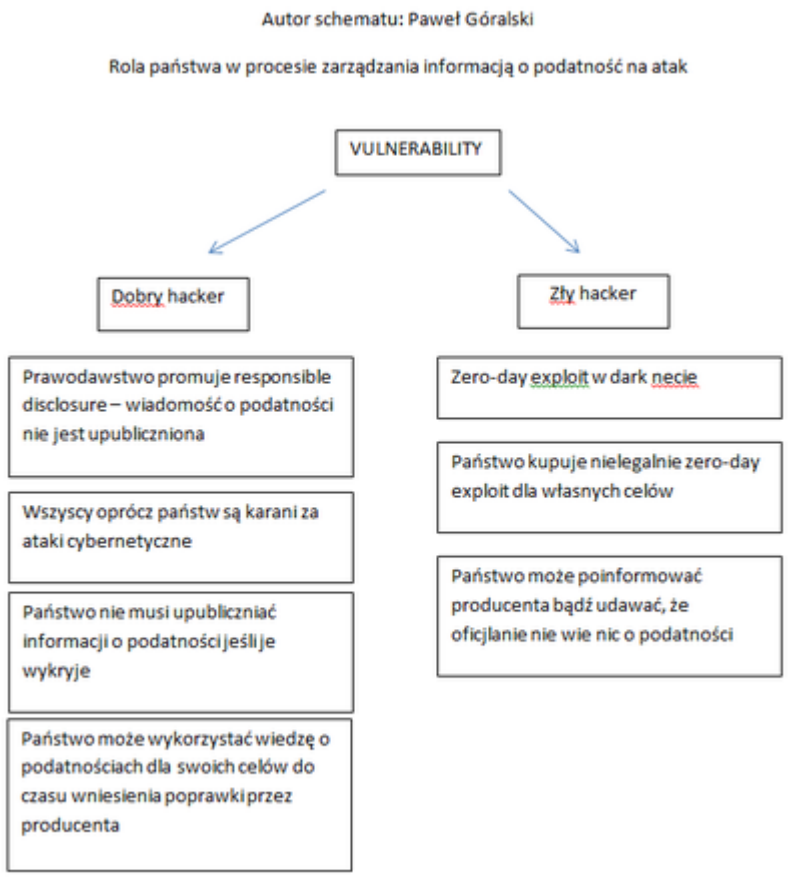
Unijne prawo co prawda zobowiązuje do wprowadzenia kar za upowszechnianie kodu dostępu, jednak w praktyce ani handel *exploitami* ani udział w nich rządów państw nie do końca został zdefiniowany. Jeżeli nielegalny atak na systemy teleinformatyczne powinien być karany, logicznie rozumując państwa powinny wzajemnie występować przeciwko sobie w trybunałach międzynadowych. Praktyka pokazuje, że jest inaczej.

W paragrafie 7 *Ustawy o Federalnym Urzędzie ds. Bezpieczeństwa w Technologiach Informatycznych* (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*) prawodawca nakłada na odkrywcę podatności obowiązek nawiązania kontaktu z producentem i nieujawniania tej informacji publicznie. Argumentem przemawiającym za takim rozwiązaniem prawnym jest zawężenie kręgu osób poinformowanych o samym zagrożeniu, tak aby nie rozpowszechniać paniki lub nie prowokować ataków ze strony black hackerów.

Powyższy przykład niemieckiego ustawodawstwa pokazuje, że państwa promują *responsibility disclosure* jako model ujawniania informacji o podatnościach. Jednak właśnie to ten model sprawia –

zdaniem przywołanego wyżej prof. dr. Hartmuta Pohla - że państwa napędzają czarny rynek *zero-day exploitów*.

Jeśli rozłożymy na czynniki pierwsze udział państwa w całym procesie, otrzymamy następujący obraz:



Fot. Paweł Góralski

Jakie jest wyjście z sytuacji

Obecnie nie istnieje optymalne rozwiązanie problemu *exploitów*. Rządy państw uczestniczą w procesie zarządzania podatnościami i trudno wyobrazić sobie model tego procesu bez ich udziału. Najprawdopodobniej takie narzędzia jak teoria gier lub zarządzanie ryzykiem pomogłyby nam lepiej zrozumieć, czy w innym schemacie da się osiągnąć optimum. Rzeczywistość pokazuje, że oba rozwiązania *full disclosure* i *responsible disclosure* pozostawiają wiele do życzenia, jeśli chodzi o efektywność.

Jeśli spróbujemy ocenić ryzyko samych procesów, dla przeciętnego obywatela nadal mniej groźne okaże się posiadanie informacji o podatnościach przez organy państwowe niż np. przez kryminalistów lub cyberterrorystów. Jak wspominaliśmy wyżej, praworządny obywatel nie powinien obawiać się państwa występującego przeciwko niemu z bronią *zero-day exploit*. Z drugiej strony, hakerzy nastawieni na korzyści materialne na pewno nie zawahają się użyć *exploitów* dla kradzieży danych czy pieniędzy itp.

Z tej perspektywy *responsible disclosure* zasługuje bardziej na poparcie niż *full disclosure*. Tej samej logice hołduje projekt Zero-day zapoczątkowany w 2014 r. przez Google. Znaleziona podatność jest przesyłana do producenta, który ma od tej chwili 90 dni na rozwiązanie problemu, w przeciwnym wypadku informacja zostanie podana do wiadomości publicznej. Ujawnienie ma spełniać w tym

wypadku rolę kija, który zmusi ostatecznie producentów do podjęcia akcji w obawie przed utratą reputacji.

Mimo wszystko pozostaje pewien niedosyt, gdy uświadomimy sobie, że to państwa podsycają wojnę cybernetyczną pozostając praktycznie poza jurysdykcją trybunałów międzynarodowych. Jak już wspomniano, pozwy z powodu ataków cybernetycznych przeprowadzonych przez rządy państw na razie nie są praktyką sądową. Brakuje ściśle sformułowanych procedur dla takich postępowań sądowych. Problem stanowi już samo zgromadzenie materiału dowodowego z wykorzystaniem informatyki śledczej (*Computer Forensics*). Wątpliwe jest przecież, aby USA pozwoliły Rosji zebrać materiały cybernetyczne dotyczące swych ataków i vice versa.

Autor : Paweł Góralski