

Ukrywane cyberataki

INTERNET | Obawiając się pozwów, firmy czasem wolą ukryć fakt włamania, a nawet zapłacić okup szantażyście, byle tylko sprawa nie ujrzała światła dziennego.

JAROSŁAW MARCZUK

Co roku polskim internetem wstrząsają głośnie włamania internetowe. Gielda, banki, lotnisko, kancelaria prawnicza już skutecznie były atakowane przez cyberprzestępców. Prawo chroni poszkodowane firmy, niestety o ich klientów w zasadzie nie dba. Nikt ich nie musi informować o tym, że ich dane wyciekły z przedsiębiorstwa i znalazły się w niepowołanych rękach. Co gorsza, z drobnymi wyjątkami, firmy nie muszą o cyberwłamaniach mówić też organom państwowym.

Istotnie niewiele

– Operatorzy telekomunikacyjni muszą zgłaszać istotne naruszenia bezpieczeństwa infrastruktury teleinformatycznej do Urzędu Komunikacji Elektronicznej – zapewnia Mirosław Maj, prezes Fundacji Bezpieczna Cyberprzestrzeń. W praktyce operatorzy nie zgłaszają wielu incydentów: drobnych włamań do swojej sieci, ataków na systemy bankowe albo na przykład prób przejęcia danych lub kontroli nad komputerami klientów. W zeszłym roku do UKE trafiły dwa zgłoszenia, w 2014 r. – pięć.

Dostawcy usług telekomunikacyjnych muszą również zawiadamiać o naruszeniu danych osobowych Generalnego Inspektora Ochrony Danych

Osobowych. W 2014 r. wpłynęło takich zgłoszeń 155, rok później 93. – Mamy absurdalną sytuację, w której operator telekomunikacyjny przetwarzający mało wrażliwe dane musi informować o ich wycieku urzędy, a podmioty z innych krytycznych sektorów gospodarki, jak szpitale czy banki, już nie mają takiego obowiązku – mówi Maj.

Ta sytuacja negatywnie odbija się również na konsumentach. – W świetle obecnie obowiązujących przepisów nie musimy zostać powiadomieni o tym, że np. w e-sklepie doszło do wycieku naszych danych osobowych – potwierdza Beata Marek, prawnik z Cyberlaw.pl.

Jedynym wyjątkiem od tej sytuacji znów są telekomunikacyjni, które muszą ostrzec abonenta lub użytkownika końcowego będącego osobą fizyczną, jeśli doszło do naruszenia danych osobowych, mogącego mieć niekorzystny wpływ na ich prawa. Firmy mają na zgłoszenie 3 dni od wykrycia incydentu, ale i tu jest mały haczyk.

– Zawiadomienie nie jest wymagane, jeżeli dostawca publicznie dostępnych usług telekomunikacyjnych wdrożył, przewidziane przepisami o ochronie danych osobowych, odpowiednie techniczne i organizacyjne środki ochrony, które uniemożliwiają odczytanie danych przez osoby nieuprawnione oraz zastosował je do danych, których ochrona została naruszona – podkreśla Małgorzata Kałużyńska-Jasak, dyrektor zespołu rzecznika prasowego GIOD.

Lepiej się nie chwalić

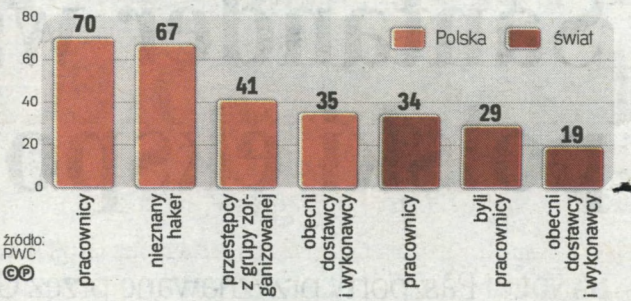
Problem najlepiej obrazuje przykład z życia wzięty. Prawie rok temu cyberprzestępca zdobył dane klientów Plus Banku i następnie część z nich opublikował w internecie. Opinia publiczna dowiedziała się o sprawie od samego złodzieja, który swoim dokonaniem podzielił się z pewnym znanym blogerem piszącym o bezpieczeństwie IT. Bank dopóki mógł, to całej sprawy się wypierał i usiłował historię zatuszować.

Co prawda złodzieja i tak udało się złapać, a GIOD nie wykryło naruszeń po stronie banku, ale jasno na tym przykładzie widać, jak bardzo niektórym firmom może zależeć na ukryciu incydentów sieciowych.

– Przedsiębiorcy, którzy padli ofiarą cyberprzestępców, często boją się do tego przyznać w obawie o utratę zaufania swoich klientów – przyznaje Marek. Nie chodzi jednak tylko o to. – Jeśli z firmowej bazy danych wypłyną dane klientów, można spodziewać się kontroli GIOD

oraz pozwów odszkodowawczych – dodaje Marek. Same GIOD nie może nakładać sankcji finansowych. Obawiając się pozwów, firmy czasem wolą ukryć fakt włamania, a nawet zapłacić okup szantażyście, ażeby sprawa nie ujrzała światła dziennego. Tym samym zachęcają kolejnych cyberprzestępców do działania. – Takie sprawy powinno się zgłaszać odpowiednim organom, bo mogą posłużyć jako okoliczność łagodząca w razie ewentualnych pozwów – twierdzi Marek. – Do bycia ofiarą ataku należy się przyznawać. Negowanie faktów

Główne źródła cyberataków, w proc.



może być po prostu groźne – zgadza się Maj.

Obowiązkowe zgłoszenia

Są szanse, że sytuacja się wkrótce poprawi. Najpóźniej w 2018 r. powinny wejść w życie regulacje wynikające z unijnej dyrektywy w sprawie bezpieczeństwa sieci i informacji. Wymusi ona na firmach zaliczanych do tzw. infrastruktury krytycznej (np. bankach i firmach energetycznych) zgłaszanie władzom informacji o udanych przeciwności atakach sieciowych. W szczególności niebezpiecznych przypadkach urzędnicy będą informować opinię publiczną o wyczynach cyberprzestępców.

Do 2018 r. zostaną również wprowadzone nowe przepisy zobowiązujące firmy do zgłaszania GIOD istotnych wycieków w ciągu 72 godzin od zarejestrowania incydentu. W tym samym czasie przedsiębiorstwo będzie musiało też powiadomić swoich klientów o zdarzeniu, jeśli atak zagrazi ich danym osobowym lub prywatności. Ponadto urząd otrzyma możliwość nakładania dotkliwych kar finansowych – do 20 mln euro lub 4 proc. rocznego światowego obrotu – na podmioty nie dbające należycie o bezpieczeństwo informacji o swoich klientach.

Niestety, obowiązek notyfikacyjny nie obejmie bowiem organów państwowych, czyli ulubionego celu cyberprzestępców. ©

masz pytanie, wyślij e-mail do autorki
j.marczuk@rp.pl