

Informacja

Strona znajduje się w archiwum.

Koszmar systemów IT w Waszyngtonie

24.03.2009 Waszyngton. Wstępne przesłuchanie głównego inspektora zajmującego się ochroną informacji Dystryktu Columbia. Yusuf Acar został zatrzymany pod zarzutem czynów korupcyjnych i pozostaje w areszcie bez możliwości wyjścia za kaucją. Podtrzymanie aresztu jest uzasadnione obawami, że na wolności mógłby mieć nadal dostęp do systemów IT Dystryktu. O sprawie doniosły media specjalizujące się w dziedzinie informatyki.

Według FBI, firma IT - Advanced Integrated Technologies Corp. (AITC), z siedzibą w Waszyngtonie, w imieniu departamentu IT Dystryktu Columbia dokonała zakupu 500 licencji od McAfee, a następnie zażądała od rządu zapłaty za 2000 licencji. Dyrektor AITC, Sushil Bansal - dyrektor AITC - był drugą osobą aresztowaną przez FBI w powiązaniu z przekrętem.

Uważa się, że technologie bezpieczeństwa zakupione za pośrednictwem AITC, niekoniecznie są najlepsze w swojej klasie i mogą nie spełniać niezbędnych wymogów. Kolejnym krokiem, chroniącym przed możliwym wyciekami informacji, jest teraz zresetowanie haseł i innych mechanizmów dostępu do bazy.

Agenci FBI znaleźli 70 tysięcy dolarów w domu Acara na przedmieściach D.C podczas aresztowania go 12 marca 2009 roku. To, co zainteresowało najbardziej agentów to fakt, że Yusuf Acar nie posiadał żadnych certyfikatów bezpieczeństwa. W jaki sposób został więc zatrudniony na stanowisku Inspektora Bezpieczeństwa Systemów Informatycznych (Information Systems Security Officer - ISSO) z wynagrodzeniem rocznym 127.468 dolarów?

W ramach swojej dotychczasowej pracy, Acar miał dostęp do danych osobowych i innych poufnych informacji zebranych w systemach D.C. Dokumenty FBI przekazane sądowi wskazują na udział również innych osób w korupcyjnej działalności. Analitycy bezpieczeństwa ostrzegają teraz, że Acar

mógł stworzyć kanały, tzw. backdoors, w systemach, pozwalające na wydostawanie się informacji, instalowanie tzw. logic bomb, czyli kodów w systemach operacyjnych, mogących dokonywać szkodliwych operacji. Ponieważ Acar przyczynił się również do niezgodnego z prawem zakupu programów zabezpieczających, zrodziło się pytanie o poziom bezpieczeństwa systemu IT w Waszyngtonie.

„Kto wie, co oni kupili? (...) Kto wie, czy nie wzięli pieniędzy za dostęp do bazy danych, albo systemu?” - zastanawia się Johannes Ullrich, Główny Inspektor Technologiczny w Instytucie SANS z Bethesdy w Maryland.

Ponieważ AITC miało również zlecenia z Biura Kadr Wydziału Komunikacji (Department of Motor Vehicles), prawdopodobnie stworzyło to spore możliwości do przejrzania zawartości baz danych, czy sprzedaży informacji o obywatelach i pracownikach. Zdaniem Alana Pallera z Instytutu SANS, istnieją obawy o to, czy działania Acara i Bansala, którzy niewłaściwie wykonywali swoje obowiązki i doprowadzili do serii zaniechań, obniżyli znacząco bezpieczeństwo systemu, skupiając się jedynie na "wypchaniu własnych kieszeni".

Opisana sprawa przekupstwa skupia na sobie więcej uwagi niż zazwyczaj, a to z powodu mianowania w ostatnim czasie, przez prezydenta - Baracka Obamę - Viveka Kundry na pierwszego w historii Głównego Inspektora Informacji w rządzie federalnym (Chief Information Officer - CIO). Vivek Kundra był do tej pory Głównym Inspektorem Technologii (Chief Technology Officer- CTO) Dystryktu. Nie istnieją jednak wskazania, według dokumentów sądowych, by Kundra posiadał jakąkolwiek wiedzę o nielegalnej działalności. Zastanawiające jest jednak to, że nowo mianowany na stanowisku CIO - Kundra, wziął w pracy wolne tzw. usprawiedliwioną nieobecność (leave of absence). Autorzy artykułu „Koszmar informatyczny w D.C. spowodowany łapówką”, opublikowanego 16 marca br. w Computer World zastanawiają się, czy w obliczu ostatnich wydarzeń, wizja o wprowadzeniu rewolucji technologicznej na szczeblu federalnym kiedykolwiek nastąpi.

Źródła: computerworld.co.nz; networkworld.com