Jak postępować, gdy ktoś wykradn[..]

2024-04-24 15:00:47

Wydruk artykułu FAQ

Kategoria:	Hosting ITL::Bezpieczeństwo	**Ostatnia aktualizacja:**	2016-04-28 09:42:17
Status:	publiczny (dla wszystkich)		
Język:	pl		

Słowa kluczowe

wirus złodziej email

Objawy (publiczny)

Ktoś wykradł mi hasło i rozsyła SPAM z mojego konta.

Problem (publiczny)

Od pewnego czasu szerzy się plaga złośliwego oprogramowania (wirusy, trojany) wykradającego hasła do kont email z komputerów osobistych. Złapany przypadkowo wirus lub zainstalowany trojan wykrada hasło z komputera Windows, z którego logowano się do konta email. Następnie inny rodzaj oprogramowania, logując się wykradzionym, prawidłowym loginem i hasłem do konta email, rozsyła SPAM.

Z punktu widzenia dostawcy usługi hostingu, serwer nie jest w stanie rozróżnić, czy operacja wysłania poczty za pomocą poprawnego loginu i hasła do konta email jest operacją osoby uprawnionej, czy też operacją przeprowadzaną przez przestępców. Loginy i hasła zabezpieczające dostęp do kont email pozostają pod kontrolą klienta - użytkownika konta email i na kliencie spoczywa obowiązek ochrony ich tajemnicy, dbania o ochronę antywirusową na swoich komputerach itp.

Rozwiązanie (publiczny)

Kolejność postępowania w przypadku stwierdzenia wycieku hasła do konta email powinna być następująca:

- Skanowanie programem antywirusowym i ewentualnie czyszczenie wszystkich komputerów, z których miało miejsce logowanie do skrzynki email, oraz wszystkich komputerów w sieciach lokalnych, skąd się logowano.
- Istnieje możliwość, że hasło zostało podsłuchane przez malware zainstalowany na routerze obsługującym połączenie internetowe. Należy sprawdzić poprawność ustawień routera (np. serwery DNS, dostęp do panelu administracyjnego - tylko z sieci wewnętrznej), zabezpieczenia. W przypadku stwierdzenia czegoś podejrzanego (lub np. niezabezpieczonego panelu administracyjnego) - należy zainstalować najnowsze oprogramowanie do routera, oferowane przez producenta, zgodnie z instrukcją. Zmiana hasła do konta email w panelu konto.itl.pl lub admin.itl.pl. W przypadku znalezienia na komputerze jakiegokolwiek wirusa, proponujemy pozmieniać wszystkie inne hasła: zarówno do kont email, kont FTP, dostępu do panelu administracyjnego, jak i np. do kont bankowych, kont w portalach społecznościowych. Proponujemy nie zapisywać haseł do konta email w programie do jego obsługi. Zalecamy włączyć protokół TLS (SSL) w połączeniach poczty wychodzącej (SMTP) i przychodzącej (POP3, IMAP).