**Jak nie stać się kolejnym Code Space**

**Zabezpiecz swoją firmę stosując się do poniższych rad odnośnie bezpiecznego używania serwisów chmurowych.**

Firma Code Spaces, która oferowała repozytoria kodów źródłowych oraz usługę zarządzania projektami dostępnymi na *Amazon's Web Services for developers*, została zmuszona do zakończenia działalności w czerwcu, kiedy to nie spełniła żądań internetowych szantażystów. Na firmę przeprowadzono atak typu DDoS (Distributed Denial of Service), po którym nastąpiło [włamanie](http://tinyurl.com/lz4dbpm) mające na celu zniszczenie całej własności intelektualnej należącej do organizacji.

Problemy firmy Code Space rozpoczęły się atakiem DDoS mającym miejsce 17. czerwca, który okazał się jedynie sposobem na odciągnięcie uwagi od włamania do systemu. Atakujący przejął kontrolę nad panelem kontrolnym Amazon EC2 i spowodował „usunięcie większości danych, wszystkich kopii zapasowych oraz danych konfiguracyjnych'', wyjaśniła firma na swoim blogu.

Podobny scenariusz może wydawać się mało prawdopodobny w odniesieniu do Twojej firmy, ale w rzeczywistości wiele dzisiejszych biznesów korzysta z usług IaaS (Infrastructure as a Service) opartych na chmurze. Umożliwia to pracownikom łatwy dostęp do danych firmowych oraz innych zasobów. Jednocześnie wiele firm nie posiada żadnych rozwiązań pozwalających na ochronę przed zagrożeniami wynikającymi z użytkowania usług IaaS, tak katastrofalnych w skutkach jak ataki DDOS i włamania do firmy Code Space. Najnowsze badania firmy Forrester Research wykazały, że tylko 57 procent firm posiada plan działania w wypadku ataku DDoS.

Możesz lepiej chronić swoją organizację przed wyżej wymienionymi zagrożeniami stosując dobre praktyki użytkowania usług IaaS.

**Zdecyduj kto powinien mieć dostęp do Twojego Panelu Zarządzania**

Udostępniając panel zarządzający chmurą IaaS wielu osobom sprawiasz, że Twój system staje się bardziej podatny na przejęcie kontroli nad całym środowiskiem - tak jak miało to miejsce w firmie Code Spaces.

Ogranicz grono użytkowników mających dostęp do panelu zarządzania do niezbędnej liczby osób aby zmniejszyć ryzyko nieautoryzowanego dostępu. Nigdy nie używaj konta root bez wyraźnej potrzeby. Utwórz konto administratora do codziennego użytku, które może zostać wykorzystane do zablokowania pozostałych użytkowników w razie ataku. W przeciwnym razie, gdy haker zdobędzie dostęp do konta root i zmieni hasło, będziesz musiał skontaktować się z dostawcą IaaS aby odzyskać kontrolę.

**Określ uprawnienia użytkowników w Panelu Zarządzania**

Zezwalaj użytkownikom jedynie na to, co jest niezbędne w ich pracy. Wygodnym sposobem organizacji uprawnień użytkowników jest utworzenie grup użytkowników i określenie dla każdej z nich minimalnych praw pozwalających na wykonanie konkretnego zadania. Potem, w trakcie dodawania nowego użytkownika, nadaj mu uprawnienia w panelu sterowania poprzez dołączenie do odpowiednich grup.

Przykładowo, utwórz grupę “Dostęp do bazy danych”. Użytkownicy w tej grupie będą mieli prawa tylko do odczytu bazy danych i nic poza tym. Będziesz musiał razem z współpracownikami poświęcić czas na ustalenie uprawnień dla każdej z grup, ale jeżeli nastąpi przejęcie konta nie mającego praw administratora, nie będzie to stanowiło zagrożenia dla całego IaaS.

**Używaj wielostopniowego uwierzytelniania**

Zaleca się wprowadzenie bardziej złożonego sposobu uwierzytelniania, aby utrudnić nieautoryzowany dostęp. Uwierzytelnianie wielostopniowe może nadal wymagać podania loginu i hasła, ale oprócz tego wprowadza weryfikację kodu dostarczanego przez usługę autoryzacyjną udostępnianą przez firmę trzecią. Kod ten może być np. generowany co minutę przez token sprzętowy albo być podany w treści SMSa wysłanego do użytkownika. Uwierzytelnianie wielostopniowe jest bezpieczniejsze niż stosowanie samego hasła.

**Rozważ stosowanie technologii SAML**

SAML, czyli Security Assertion Markup Language, to otwarty standard, który może być wykorzystywany wraz z innymi mechanizmami identyfikacji jak np. Windows Active Directory Federation Services. Możesz włączyć w panelu sterowania używanie Windows Active Directory w celach identyfikacji. W ten sposób dodawana jest kolejna warstwa bezpieczeństwa, która pozwala użytkownikom logować się do panelu sterowania jedynie gdy przebywają w sieci firmowej lub w zabezpieczonej sieci VPN, która wymaga logowania przez Active Directory.

**Zadbaj o bezpieczeństwo sieci firmowej**

Poprzez wprowadzenie zabezpieczeń w sieci firmowej zminimalizujesz ryzyko infekcji koniami trojańskimi lub innym złośliwym oprogramowaniem, które może przechwycić dane logowania użytkownika. Upewnij się, że oprogramowanie antywirusowe jest aktualizowane na bieżąco i skanuje komputery w regularnych odstępach czasu. Zainstaluj sieciowy firewall oraz systemy IPS (Intrusion Prevent System) aby jeszcze bardziej wzmocnić ochronę. Rozważ również kupno sieciowego oprogramowania antywirusowego i anty-botowego, a także rozwiązań emulujących zagrożenia, by być przygotowanym na nowe, nieznane rodzaje ataków.

**Opracuj scenariusze kryzysowe na wypadek utraty danych**

Niezbędnym minimum dla Twojej firmy jest opracowanie trzech scenariuszy pozwalających na zminimalizowanie utraty danych i przerw w dostępie do oferowanych przez Ciebie usług.

**\*Scenariusz dla ataków typu DDoS**, który określa jakie kroki należy podjąć, gdy taki atak nastąpił.

**\*Scenariusz dla incydentów bezpieczeństwa**, który opisuje postępowanie na wypadek różnych typów włamań do sieci firmowej

**\*Scenariusz ciągłości dostaw usług**, który przedstawia jakie kroki powinna podjąć Twoja firma, aby zminimalizować przerwy w dostępie do usług w przypadku wystąpienia incydentu bezpieczeństwa

Aby lepiej i szybciej opracować te plany, przeczytaj [AWS Security Best Practices](http://aws.amazon.com/whitepapers/aws-security-best-practices/) oraz dokumenty National Institute of Standards and Technology (NIST) - [“Computer Security Incident Handling Guide”](http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf) oraz [Techniques for System and Data Recovery](http://www.nist.gov/manuscript-publication-search.cfm?pub_id=51024).”

Oczywiście jedynie przygotowanie tych planów jest niewystarczające. Należy również sprawdzić skuteczność działania tych planów poprzez regularne testowanie – tak samo jak regularnie przeprowadza się próbną ewakuację przeciwpożarową w wielkich biurowcach.

**Chroń IaaS tak jak swój własny serwer**

Konfigurując środowisko w AWS lub innej usłudze IaaS, powinieneś chronić serwery w taki sam sposób, jak gdyby znajdowały się w Twojej firmie. Firma Check Point oferuje [bramę bezpieczeństwa w sklepie Amazon Marketplace](https://aws.amazon.com/marketplace/pp/B00CWNBJOY/ref=srh_res_product_title?ie=UTF8&amp;amp;sr=0-2&amp;amp;qid=1404328482628), która pozwoli Ci na wprowadzenie reguł bezpieczeństwa wymaganych przez Twoją firmę, aby uchronić zasoby znajdujące się w środowisku AWS.

W sklepie Amazon Marketplace oferowane są takie same środki bezpieczeństwa jak dla sieci firmowych. Dzięki temu, Twoja usługa IaaS może być bezpiecznie połączona z Twoją siecią firmową za pomocą VPN. Masz wtedy pewność, że IaaS posiada dokładnie taki sam poziom zabezpieczeń jak sieć firmowa.

Łatwość i dostępność ofert IaaS to ogromne korzyści dla wielu przedsiębiorstw, jednak każda firma powinna zadbać o zachowanie odpowiedniej równowagi pomiędzy spełnianiem wymagań użytkowników a bezpieczeństwem swoich danych.

W Polsce dystrybutorami produktów Check Point są firmy Clico Sp. z o.o. ([www.clico.pl](http://www.clico.pl/)) oraz RRC Poland Sp. z o.o. ([www.rrc.pl](http://www.rrc.pl/)).