**50 procent baz danych firm narażonych na niepowołany dostęp. Powód: luki w zabezpieczeniach rozwiązań chmurowych**

**Kwestia bezpieczeństwa danych przetrzymywanych w chmurze to poważny problem coraz większej ilości przedsiębiorstw. Badanie Bitdefender wykazało, że tylko jedna na sześć firm szyfruje całość swoich danych. 85 procent ankietowanych dyrektorów ds. bezpieczeństwa obawia się luk w zabezpieczeniach jeśli chodzi o publiczne rozwiązania chmurowe.**

Dokładnie 51 procent przedsiębiorstw nie chroni w odpowiedni sposób danych przetrzymywanych na dyskach wirtualnych narażając je tym samym na ryzyko niepowołanego dostępu np. ze strony hakerów, jak podaje RedLock.

Jeszcze w zeszłym miesiącu 48 milionów prywatnych profili zebranych przez LocalBox (w celu świadczenia usług reklamowych) z takich portali jak Facebook, LinkedIn i Twitter było narażonych na niepowołany dostęp każdego użytkownika Internetu. Wszystko przez błędy w konfiguracji rozwiązań chmurowych dostarczanych przez firmę Amazon (Amazon Web Services). Nie był to jedyny przypadek, gdyż Pentagon, Tesla, Verizon oraz Dow Jones również ucierpiały w wyniku wycieku danych spowodowanym przez luki bezpieczeństwa w posiadanych przez siebie chmurach.

„Przechowywanie danych w chmurze daje ogromną elastyczność i wygodę”, komentuje Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken, „Niestety te zalety tracą całą swoją wartość bez odpowiedniego zabezpieczenia serwera” – dodaje.

Jedna, wrażliwa aplikacja na serwerze to wszystko czego potrzebują cyberprzestępcy, aby uzyskać dostęp do jego infrastruktury i przejąć go. Tylko w zeszłym roku 51 procent przedsiębiorstw nie chroniło w odpowiedni sposób danych przetrzymywanych w chmurze, informuje RedLock. Firmy są entuzjastycznie nastawione wobec rozwiązań chmurowych, gdyż umożliwiają im przechowywanie dużej ilości danych mniejszym kosztem. Pomimo tego, że firmy powszechnie wdrażają usługi cloud, jeszcze bardziej narażają swoje bezpieczeństwo

i prywatność danych. Przypadków cryptojackingu w drugim kwartale 2018 było o 8 procent więcej; aż 25 procent przedsiębiorstw zgłosiło tego typu atak.

Niektóre serwery nie są nawet chronione hasłem, nie wspominając o bardziej zaawansowanych metodach zabezpieczeń i to jest prawdopodobnie powód tego, że 27 procent firm takich jak Uber, Tesla, OneLogin, Aviva, i Gemalto zgłosiło naruszenie wrażliwych danych swoich klientów, podaje RedLock. Co więcej, 24 procent przedsiębiorstw jest narażonych na poważne zagrożenia bezpieczeństwa, z racji tego, że serwery ich danych w chmurze nie posiadają odpowiednich aktualizacji. W ciągu ostatnich 12 miesięcy luki bezpieczeństwa w chmurach zagroziły takim firmom jak MongoDB, Elasticsearch, Intel czy Drupal.

„Rozumiemy na czym polega problem niekończących się raportów dot. infrastruktur IT, którym brakuje prawidłowej ochrony. Mamy dowody na to, że korporacje podejmują inicjatywy, aby ograniczyć ilość swoich słabych punktów, ale do zrobienia w tej kwestii jest

o wiele więcej”, powiedział Guarav Kumar, dyrektor ds. technologii w RedLock.

Bazy danych przedsiębiorstw nie są poprawnie zaszyfrowane. Sektor biznesowy nie potrzebuje specjalnych badań, żeby to stwierdzić, ale pewnego rodzaju potwierdzenie wydaje się potrzebne. Chociażby po to, aby więcej firm posiadało świadomość zagrożenia. Nowa ustawa o ochronie danych osobowych jest ważnym czynnikiem, przez który przedsiębiorstwa zadbają, aby ich sieci były wolne od ataków i wycieków danych.