Rejestracja czasu pracy w chmurze, czyli RCP i KD w jednym

Bezpieczeństwo i koszty

Daniel Hat
HatPol

Im więcej poznawałem i używałem KD i RCP w chmurze, tym bardziej mnie to rozwiązanie zachwycało; poznałem elastyczność, wygodę i bezpieczeństwo serwisu GuardSaas.

Szybka definicja chmury
Najpopularniejsze tego typu usługi to chmura obliczeniowa oraz tzw. dysk w chmurze. Wiele rozwiązań, z których korzystamy na co dzień, jest rozpowszechnianych przez potentatów z branży IT (Microsoft, Google, Apple i in.). W skrócie, chmura jest dla naszych danych pewnego rodzaju serwerem, czyli przestrzenią udostępnianą nam przez dostawcę za pośrednictwem internetu, do której mamy dostęp z dowolnego komputera, tabletu czy smartfonu z poziomu przeglądarki lub za pomocą specjalnej aplikacji. Warto zaznaczyć, że rozwiązanie to jest bardzo popularne i ma wiele zastosowań. Z tego typu usług korzystają miliony ludzi na całym świecie.

Co chmura ma wspólnego z kontrolą dostępu i rejestracją czasu pracy?

Wielu autorów publikacji wyjaśniło termin „serwis w chmurze" i sklasyfikowało tę technologię, próbując określić tendencję jego rozwoju. Jednak jeśli chodzi o nośniki w branży bezpieczeństwa, to żaden wydawca ani portal nie porusza kwestii usług w chmurze dla kontroli dostępu. Przynajmniej ja, dość intensywnie śledząc branżę kontroli dostępu, nigdy nie napotkałem podobnego artykułu.

Z upływem czasu większość branży zabezpieczeń przyzwyczaiła się do nowego terminu i dostępności nowych technologii. Mimo to niektóre z zagadnień związanych z usługami w chmurze, w tym dziedzina kontroli dostępu, są słabo znane. Dlatego uważam, że należy poruszyć ten temat i opisać działanie chmury dla RCP i KD.

Myślę, że zazwyczaj problemy deweloperów i obiekcje inwestorów są związane z bezpieczeństwem danych i kosztami usługi. Dlatego w tym artykule nie będę zajmować się zagadnieniami typu, „czy istnieje życie na Marsie", ale stwierdzam fakt: usługi w chmurze dla systemów zabezpieczeń i rejestracji czasu pracy istnieją, są funkcjonalne, wykonują określone zadania i mają dużą grupę klientów. Postaram się odpowiedzieć na najczęściej zadawane pytania na temat bezpieczeństwa i kosztów usług w chmurze, korzystając z ogólnej wiedzy, ale także w oparciu o doświadczenia dotyczące jednej z istniejących usług RCP i KD w chmurze. Początkowo, poznawszy takie zestawienie, byłem sceptycznie nastawiony, jednak im więcej poznawałem i używałem KD i RCP w chmurze, tym bardziej mnie to rozwiązanie zachwycało; poznałem elastyczność, wygodę i bezpieczeństwo serwisu GuardSaas.

Zapewne wielu inżynierów z branży nie słyszało o takim rozwiązaniu i nie może sobie wyobrazić, jak działa równocześnie rejestracja czasu pracy oraz kontrola dostępu obiektów przez chmurę. Usługa GuardSaas, o której mowa, to nic innego, jak strona www z serwerem, która za pomocą konwertera łączy się z kontrolerami i pobiera rejestry, po czym je segreguje, tworzy raporty, harmonogramy, itp. Dostęp do tego wszystkiego ma administrator lub użytkownik z uprawnieniami z dowolnego miejsca na świecie, używający dowolnego urządzenia z dostępem do internetu i przeglądarką www.

Bezpieczeństwo usługi w chmurze dla systemów kontroli dostępu

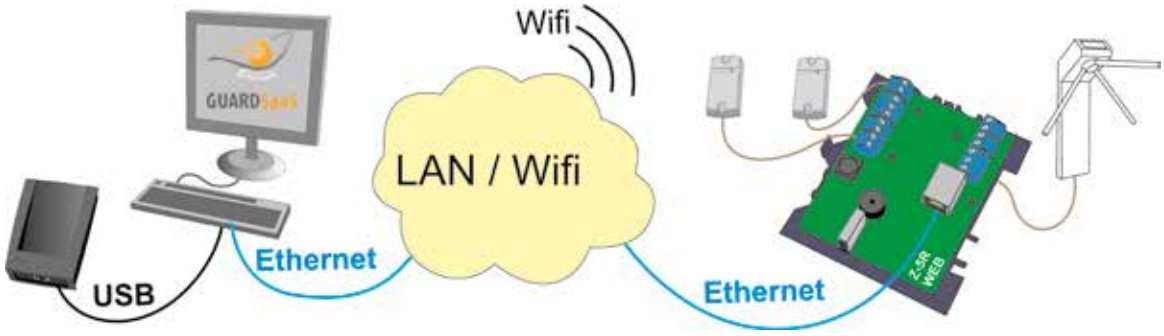
Kwestia bezpieczeństwa danych w chmurze zwykle sprowadza się do trzech zagadnień:

1. Dane z systemu kontroli dostępu są przechowywane na serwerze zdalnym. Co jeżeli serwer przestanie działać? Co zrobić, jeśli wszystkie dane z systemu kontroli dostępu będą z jakiegoś powodu usunięte?

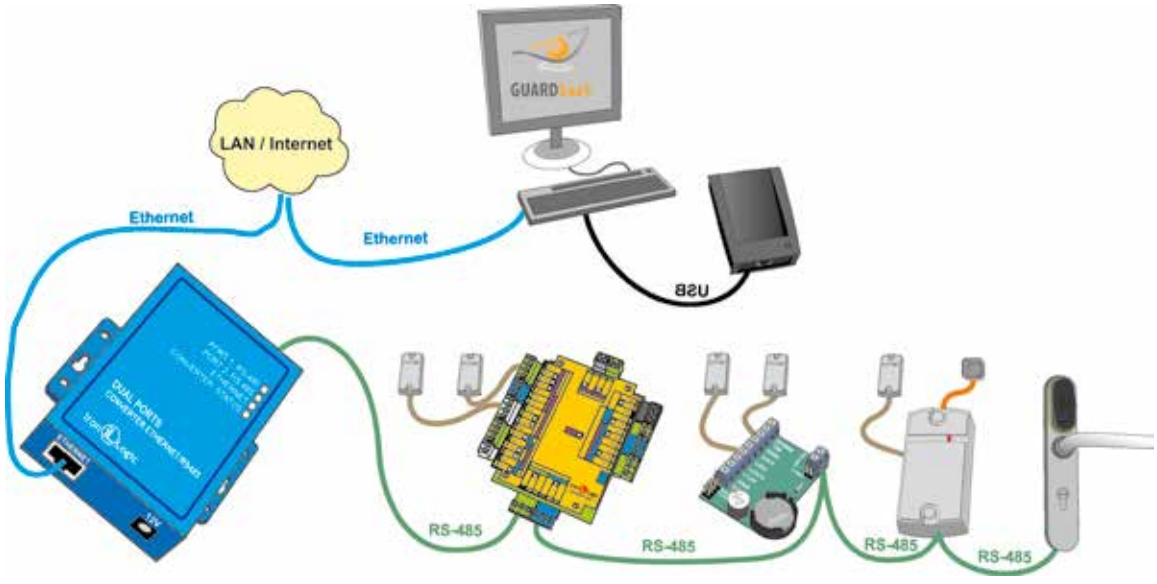
2. Co będzie, jeśli urządzenia kontroli dostępu stracą połączenie z internetem?

3. Informacje z kontroli dostępu znajdują się gdzieś w cyberprzestrzeni. Czy oznacza to, że dostęp do nich może uzyskać każdy?

Po kolei. Jeśli chodzi o utratę danych z powodu awarii serwera, należy zauważyć, że usługi szanującego się dewelopera chmury będą działać tylko z zaufanym dostawcą, który przeprowa-



Konfiguracja GuardSaaS z niezależnym kontrolerem Z5R-WEB



Konfiguracja GuardSaaS z konwerterem Z397-WEB

Sytuacja	Zachowanie programu KD, który jest zainstalowany na komputerze	Zachowanie KD zainstalowanego w chmurze
Awaria dysku twardego	Informacje, które zostały zapisane na twardym dysku, trudne do odzyskania.	Informacje będą przechowywane przez tworzenie kopii zapasowych.
Kradzież lub przejęcie komputera	Informacje te generalnie nie mogą zostać przywrócone.	Informacje te pozostają na serwerze zdalnym.
Przypadkowe lub celowe skreślenia pracowników	Informacje te nie mogą zostać przywrócone	Informacje będą przechowywane przez kopie zapasowe. Możliwe jest również, aby prawa dostępu do programu miały tylko wyznaczone osoby, np. dyrektor.

dza regularne monitorowanie serwera. W związku z tym prawdopodobieństwo awarii serwera jest zminimalizowane. Ponadto twórcy chmury zastrzegają sobie procedurę serwisową i regularnie są tworzone kopie zapasowe, które dają gwarancję bezpieczeństwa danych, nawet w razie wystąpienia problemów z serwerem.

Jeżeli chodzi o kwestię funkcjonowania systemu z tymczasową utratą łączności z internetem, specyfiką usługi GuardSaas podczas pracy z kontrolą dostępu i rejestracją czasu pracy jest to, że urządzenia działają niezależnie od połączenia z internetem. Oznacza to, że połączenie z serwerem może zostać utracone i nie jest to żaden problem, ponieważ zdarzenia nadal są zapisywane w buforze urządzeń i kiedy znów zostanie nawiązane połączenie, serwis automatycznie zaktualizuje dane (logi), pobierając je z kontrolerów. Tak więc korzystanie z usługi GuardSaas w przypadku chwilowego załamania komunikacji jest całkowicie bezpieczne.

Następnie należy rozważyć stwierdzenie, że dane przechowywane w chmurze mogą być przejęte przez hakerów. W tej kwestii głównym argumentem na korzyść chmury jest to, że wymiana danych z serwerem odbywa się za pośrednictwem bezpiecznego protokołu HTTPS, który obsługuje szyfrowanie. Jak wiadomo, z tego protokołu korzysta wiele szanujących się instytucji, np. banki. HTTPS chroni przed atakami na połączenia sieciowe. Dlatego przechwytywanie danych z RCP i KD podczas pracy w chmurze jest niezwykle trudne. Jeżeli jakaś instytucja będzie obawiać się o dane RCP w chmurze, powinna zamknąć rachunek bankowy i przechowywać pieniądze we własnym sejfie. Dla takich inwestycji również będzie stworzona kolejna wersja GuardSaaS, przygotowana do instalacji na wewnętrznym serwerze Unix.

Odnośnie włamań w urządzenia kontroli dostępu (kontrolery, konwertery) istnieje sposób, który rozwiązuje ten problem. Na przykład sprzęt marki IronLogic, który współpracuje z usługami w chmurze, jest wyposażony w przełącznik sprzętowy, który po przełączeniu (zamknięciu) chroni system przed jakimikolwiek zmianami i równocześnie pozwala czytać karty oraz przesyłać informacje o zdarzeniach. Oznacza to, że nawet w razie złamania hasła do urządzeń, atakujący nie będzie mógł wprowadzić zmian w urządzeniach, ponieważ ich pamięć będzie fizycznie zablokowana, a każda próba skasowania ustawień nie będzie możliwa. Uważam, że fizyczne zabezpieczenie sprzętu jest najbezpieczniejszym rozwiązaniem w ochronie danych w kontroli dostępu z usługą w chmurze.

Jeszcze kilka słów o niezawodności usług w chmurze dla RCP i KD. Jest to porównywalne do niezawodności przechowywania danych na standardowym oprogramowaniu zainstalowanym w komputerze użytkownika. Jak przedstawiono w tabeli, serwis w chmurze może zapewnić większe bezpieczeństwo i ochronę danych niż standardowy program KD zainstalowany na komputerze biurowym.

Koszt eksploatacji usług RCP i KD w chmurze

Czasami słyszę, że korzystanie z usług w chmurze jest droższe niż zakup klasycznej licencji na stacjonarny komputer. Być może to błędne przekonanie wzięło się stąd, że twórcy usług chmury dla systemów zabezpieczeń oferują dożywotni zakup licencji, ale również, jako opcję, udostępniają możliwość jego czynszowego opłacania. Opcje najlepszego sposobu płatności za korzystanie z usług w chmurze wykraczają poza ramy tego artykułu, gdyż uważam, że wybór metody nabycia praw własności do programu zależy od konkretnych zadań obiektów i od użytkowników.

Dla zobrazowania kosztu oprogramowania do kontroli dostępu wziąłem klasyczny program i usługi w chmurze. Otrzymałem następującą sytuację: jeśli planowane jest zainstalowanie systemów zabezpieczeń w jednym obiekcie, to zakup licencji na program klasyczny czy usługę w chmurze będzie podobny. Natomiast jeśli plan instalacji dotyczy kilku obiektów, które są daleko od siebie, a chcemy połączyć owe obiekty w jedną sieć, tańszą opcją jest RCP w chmurze.

Tak więc jeśli jednym z głównych kryteriów przy wyborze oprogramowania jest ekonomia, w przypadku instalowania KD na jednym obiekcie nie ma wielkiej różnicy, jakie zostanie użyte oprogramowanie: klasyczne lub w chmurze. W przypadku montażu pojedynczego obiektu wybór może zależeć od funkcjonalnej wygody pracy i mobilności oprogramowania. Jeśli potrzebujesz systemu do tworzenia sieci wielu obiektów (sieć sklepów, magazynów itp.), to najtańszym rozwiązaniem jest skorzystanie z usługi w chmurze.

Przykład zastosowania usługi KD w chmurze

Najlepszym przykładem zastosowania oprogramowania GuardSaas jest wykorzystanie rozwiązania do innego celu niż jego początkowe przeznaczenie. Właściciel 75 bankomatów zamontował zestaw: Z5R-WEB + CP-Z2M do każdego z bankomatów, jako dodatkowe zabezpieczenie. Każdy uprawniony ochroniarz jest wyposażony w zwykły klucz oraz w kartę zbliżeniową. Wszystkie kontrolery Z5R-WEB są wpięte do internetu i pobierają dane w czasie rzeczywistym. Dzięki takiemu rozwiązaniu właściciel bankomatów ma podwójne zabezpieczenie oraz rejestry zapisane w bazie danych, do których ma wgląd z każdego miejsca na świecie, i wie, który pracownik o której godzinie i w którym bankomacie przeprowadzał serwis.

Mam nadzieję, że ten artykuł pomógł rozwiać obawy instalatorów oraz inwestorów do usług w chmurze, co przyczyni się do prawidłowego wyboru systemu. Rynek elektronicznej kontroli dostępu nie dopracował się jeszcze jednego standardu pracy, dlatego pojawienie się nowych technologii rozszerza gamę sposobów budowania systemów zabezpieczeń i zapewnia nowe możliwości, co niewątpliwie będzie miało pozytywny wpływ na rozwój całej branży.