Przegląd cyberbezpieczeństwa CathexisVision 2020

Spis treści

1 Wprowadzenie[1]

Firma Cathexis od ponad 20 lat opracowuje i dostarcza na rynek globalny rozwiązania do zarządzania sygnałem wizyjnym. Bezpieczeństwo związane zarówno z dostępem do danych, jak i ich integralnością, zawsze stanowiło wysoki priorytet, biorąc pod uwagę bezpieczne środowisko, w którym produkty Cathexis były używane.

W ostatnim czasie termin "Cyberbezpieczeństwo" stał się gorącym tematem w dziedzinie systemów bezpieczeństwa fizycznego i jest czymś, co firma Cathexis traktuje bardzo poważnie.

W niniejszym dokumencie przedstawiono środki zastosowane w celu zmniejszenia ryzyka dostępu do informacji i manipulacji danymi, a także przedstawiono sugestie dotyczące zwiększenia bezpieczeństwa w obszarach systemów, których Cathexis nie może kontrolować, takich jak urządzenia peryferyjne i sprzęt innych firm.

[1] Chociaż firma Cathexis dołożyła wszelkich starań, aby zapewnić dokładność tego dokumentu, nie ma żadnej gwarancji dokładności, ani wyraźnej, ani dorozumianej. Dane techniczne mogą ulec zmianie bez powiadomienia.

2 Bezpieczeństwo Cathexis

W tym rozdziale przedstawiono różne środki bezpieczeństwa podejmowane przez Cathexis.

2.1 Komunikacja między komponentami CathexisVision

System CathexisVision zapewnia bezpieczną komunikację między swoimi komponentami, w tym:

i. Serwery nagrywające do klientów,
ii. Serwery nagrywające do innych serwerów nagrywających,
iii. Serwery nagrywające do Ścian Wizyjnych,
iv. Serwery zapisu do bramek zarządzania alarmami.

Bezpieczna komunikacja pomiędzy powyższymi komponentami powinna być zapewniona przez:

i. Wszystkie połączenia ze stronami zewnętrznymi obsługują szyfrowanie o różnym poziomie:
    a. Wyłączone,
    b. Minimalny (szyfrowane są tylko połączenia krytyczne),
    c. Secure (opcja domyślna, która szyfruje wszystkie połączenia z wyjątkiem tych z dużą ilością wideo),
    d. All (wszystkie połączenia szyfrowane, w tym połączenia wideo o dużej objętości).
ii. Hasła nigdy nie są przechowywane jako zwykły tekst, a zamiast tego są haszowane przy użyciu SHA512 (z CathexisVision 2017).
iii. Dane uwierzytelniające logowania są negocjowane przy użyciu wymiany kluczy Diffie-Hellmann i podpisywane kluczem prywatnym RSA (obsługuje klucze RSA 1024 i 2048).
iv. Szyfrowanie na kanałach sieciowych odbywa się przy użyciu AES128/GCM z unikalnymi kluczami szyfrującymi negocjowanymi dla każdego połączenia.
v. HMAC jest używany do weryfikacji integralności.
vi. Infrastruktura klucza publicznego (PKI) jest zarządzana wewnętrznie przez firmę Cathexis w celu zwiększenia bezpieczeństwa.

2.2 Archiwizacja danych

i. Integralność nagrań wideo jest zabezpieczona przy użyciu podwójnych kluczy RSA1024 (do podpisywania),
ii. Opcjonalne szyfrowanie odbywa się przy użyciu szyfrowania blokowego AES128 z losowym kodem IV na blok i hasłem generowanym przez użytkownika.
iii. Wideo może zawierać znacznik autoryzacji w celu wskazania źródła informacji (np. informacji o użytkowniku).
iv. Materiał wideo i metadane mogą być odtwarzane wyłącznie za pomocą zastrzeżonego odtwarzacza wideo Cathexis Archive.
v. Odtwarzanie wyeksportowanych/zarchiwizowanych materiałów wideo może być ograniczone do odtwarzania pod kontrolą hasła.

2.3 Ochrona danych osobowych (POPI)

W celu zapewnienia, aby materiał wideo nie przedostał się do domeny publicznej, dodaliśmy możliwość:

i. Archiwizowania materiałów wideo, które mogą być odtwarzane tylko pod kontrolą hasła.
ii. Nałożenie na wideo znacznika autoryzacji w celu pokazania źródła informacji (np. informacji o użytkowniku).

3 Urządzenia peryferyjne

Różnorodność produktów i protokołów, z którymi łączy się CathexisVision, decyduje o bezpieczeństwie urządzeń peryferyjnych (np. kamer IP). Z tego powodu firma Cathexis współpracuje z partnerami technologicznymi i innymi podmiotami branżowymi w celu zwiększenia bezpieczeństwa tego interfejsu.
Ogólnie rzecz biorąc, połączenie z kamerami IP obejmuje następujące czynności:

3.1 Konfiguracja kamery

i. HTTP: protokół hipertekstowy,
ii. Szyfrowany ssl/tls,
iii. Obsługiwany przez CURL (client-side URL transfer library).

3.2 Sterowanie kamerą

i. RTSP - protokół strumieniowania w czasie rzeczywistym.
ii. Sterowanie połączeniem z kamerą szyfrowanym protokołem HTTPS (jeśli jest obsługiwane przez producenta).

3.3 Strumieniowe przesyłanie obrazu wideo

i. RTP - protokół transportowy czasu rzeczywistego.
ii. Szyfrowana transmisja strumieniowa wideo (o ile jest obsługiwana przez producenta).

4 Czynniki związane z technologią informacyjną

W tej części omówiono kwestie bezpieczeństwa związane z systemem informatycznym, na które Cathexis nie ma wpływu.

4.1 Dostęp do sieci

Pierwszym krokiem w każdym systemie jest zapewnienie odpowiedniej kontroli dostępu do sieci. Istnieją w tym celu różne techniki, które są dobrze udokumentowane i powinny być znane i stosowane przez każdą kompetentną firmę sieciową. Obejmują one:

i. Zapory sieciowe,
ii. Inteligentne przełączniki sieciowe,
iii. Sieci zarządzane,
iv. Kontrola "fizycznego" dostępu do sieci.

4.2 Blokada systemu operacyjnego

W celu zaatakowania oprogramowania, dostęp uzyskiwany jest poprzez system operacyjny systemu, na którym działa oprogramowanie. Dlatego ważne jest, ”zablokowanie” systemu operacyjnego, aby zapobiec nieautoryzowanemu dostępowi. Można to zrobić na kilka sposobów, w tym:

i. Zapobieganie otwieraniu nieautoryzowanych portów umożliwiających korzystanie z elementów takich jak ftp, telnet, email. Jeśli jakakolwiek komunikacja musi odbywać się za pośrednictwem tych środków, należy upewnić się, że wykorzystywane są protokoły bezpieczeństwa, takie jak SSH/SFTP,
ii. Wyłączenie dostępu "root" do systemu operacyjnego,
iii. Zapewnienie wysokiego poziomu haseł,
iv. Dodanie oprogramowania antywirusowego i anty-malware, które jest stale aktualizowane,
v. Ograniczenie dostępu do Internetu.

5 Wnioski

Więcej informacji można uzyskać na stronie internetowej CathexisVision (www.cathexisvideo.com) lub pod adresem support@cat.co.za.