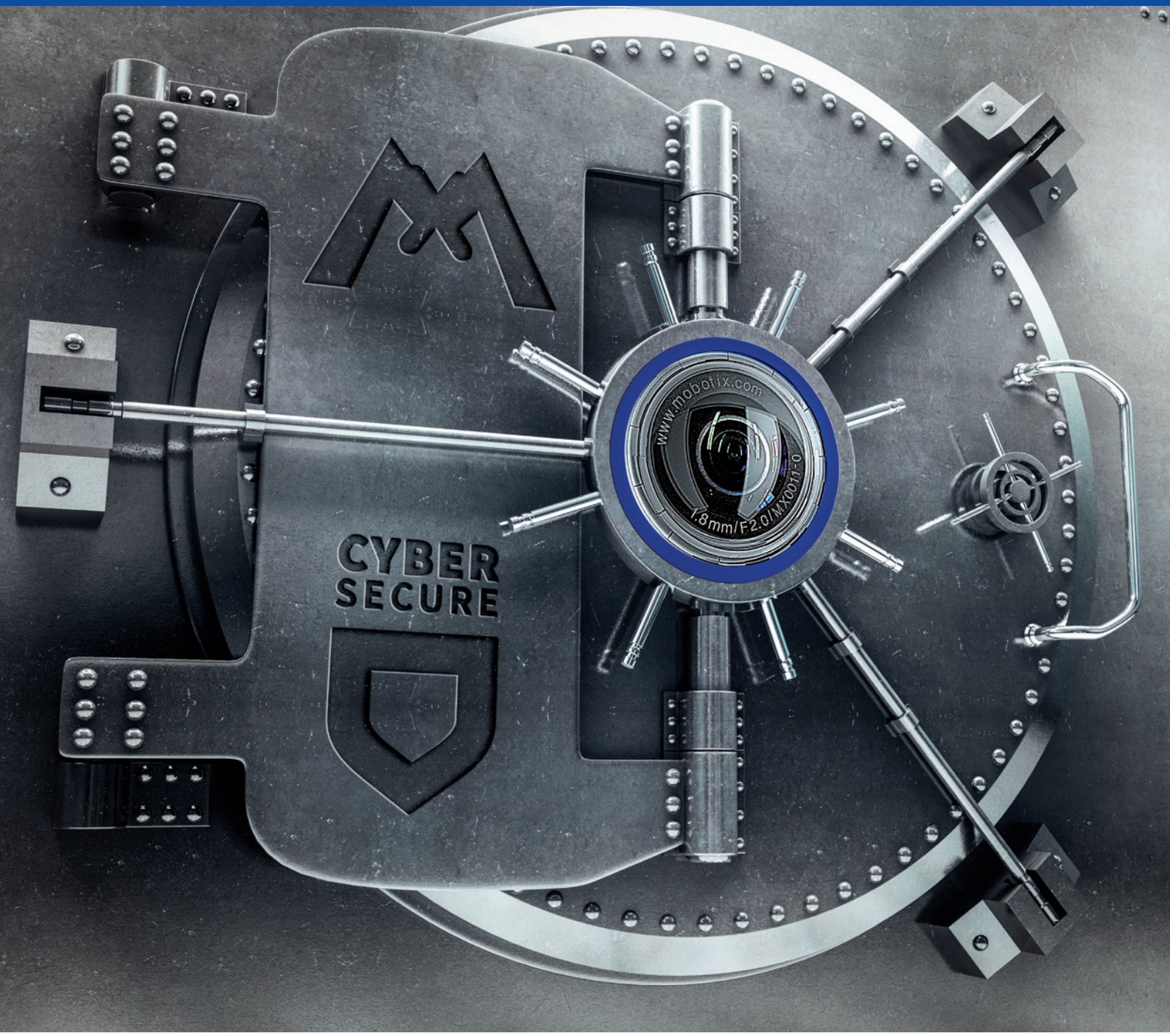
Znaczenie cyberzabezpieczeń w systemach monitoringu wideo

Artykuł przeglądowy



BeyondHumanVision

MOBOTIX

Wprowadzenie

Zastosowanie wideo w zakresie ochrony, kontroli przemysłowej, służby zdrowia i bezpieczeństwa przynosi korzyści miliardom ludzi każdego dnia. Od rodzin, które spacerują po bezpiecznym centrum handlowym pod czujnym okiem kamer CCTV, przez zdalne wideo pomagające kierownictwu w wykrywaniu wad na linii produkcyjnej, po troskliwych rodziców monitorujących dziecko podczas snu – monitoring wideo jest obecny w życiu nas wszystkich.

Najważniejsze czynniki wzrostu popularności		
1	Wzrost obaw o bezpieczeństwo	58%
2	Udoskonalenia analizy wideo	51%
3	Dostępność sieci IP	50%

Do wzrostu popularności wideo w monitoringu i innych zastosowaniach przyczyniają się szeroko pojmowane sektory informacji, komunikacji i technologii. Dawniej monitoring wymagał człowieka-operatora, który musiał obejrzeć i ocenić daną sytuację. Obecnie obraz wideo coraz częściej jest powiązany z innymi typami danych rejestrowanych przez czujniki, np. czujniki temperatury, dźwięku czy ruchu, oraz z systemami sztucznej inteligencji, które potrafią automatycznie generować alarmy lub aktywować określone działania. Wideo nie jest już jedynie sposobem na bierne rejestrowanie obrazu, lecz staje się podstawą dla bardziej zautomatyzowanych systemów, wykonujących określone zadania na podstawie zaobserwowanych sytuacji.

Od prostych rozwiązań, takich jak rozpoznawanie tablic rejestracyjnych w systemach opłat drogowych, po bardziej zaawansowane narzędzia, które potrafią wizualnie wykrywać drobne usterki maszyn przed ich całkowitą awarią – te przykłady to zaledwie czubek góry lodowej. Nawet w powszechnie stosowanych aplikacjach, takich jak monitoring sklepowy, nowoczesne technologie wprowadzają dodatkowe elementy, np. zliczanie ludzi i analizę wzorców zakupowych, które pomagają w rozmieszczeniu półek w sklepie, a nawet w projektowaniu nowych centrów handlowych.

Zapotrzebowanie rośnie – jak szacuje firma Cisco, do roku 2020[1] wideo związane z rozrywką i biznesem będzie stanowiło 79% ruchu w Internecie. Mniejsze, tańsze i bardziej energooszczędne kamery sprawiają też, że tworzenie nagrań wideo jest coraz łatwiejsze. Również przesyłanie wideo ze źródła do punktu docelowego staje się mniej złożone z uwagi na powszechną dostępność łączy internetowych i szybszych sieci komórkowych. Wideo – a zwłaszcza monitoring wideo – jest w dużej mierze postrzegane jako ważna korzyść dla społeczeństwa, ponieważ pomaga zmniejszać przestępczość i zwiększać swobodę osobistą dzięki poprawie bezpieczeństwa. Wraz z rozpowszechnieniem systemów wideo stają się one jednak coraz bardziej narażone na ataki przestępców, terrorystów i innych grup, które chcą zakłócić działanie platform monitoringu lub wykorzystać je do własnych, bezprawnych celów.

Ryzyko: brak zabezpieczeń monitoringu wideo i urządzeń IoT

Dawniej ataki na sieci monitoringu wideo były rzadkością. Wynikało to z zamkniętego charakteru systemów, które często były połączone z pomieszczeniem kontrolnym w budynku za pomocą prywatnych, bezpośrednich sieci kablowych. Starsze kamery wideo były obsługiwane w zasadzie sprzętowo i wyposażone w bardzo proste oprogramowanie wbudowane, umożliwiające niewiele więcej niż przesłanie wideo przez kabel koncentryczny. Wszystko to zdecydowanie ograniczało możliwości ich zaatakowania. Czasy się jednak zmieniają. Nowoczesne kamery wideo są właściwie komputerami, dysponującymi oprogramowaniem i cyfrowym przetwornikiem obrazu. Z uwagi na wzrost powszechności Internetu i spadek cen kamer systemy monitoringu wideo są coraz częściej dostępne za pośrednictwem dowolnej sieci IP.

Złożoność i zmieniający się charakter procesów, protokołów oprogramowania i mechanizmów uwierzytelniania sprawiają, że liczba luk będzie wzrastać – podobnie jak liczba ataków ukierunkowanych często na wydobycie danych kart kredytowych lub innych cennych informacji z systemów detalistów i usługodawców. Sam problem nie jest niczym nowym. Analitycy zabezpieczeń[2] od ponad dziesięciu lat wykrywają w kamerach luki, które dotyczą zarówno dużych dostawców międzynarodowych, jak i mniejszych marek regionalnych. Lista problemów jest coraz dłuższa i obejmuje:

- Ataki, w wyniku których przestępcy zdobywają hasło administratora urządzenia, pokonując zabezpieczenia z poziomu konta użytkownika domyślnego
- Eksploity, które omijają uwierzytelnianie użytkowników, wykorzystując dane uwierzytelniające zakodowane sprzętowo jako „furtka” przez producenta urządzenia
- Wykonanie dowolnego kodu na urządzeniu bez uwierzytelnienia przez wykorzystanie luk w module obsługi pakietów w protokole RTSP
- Luki w zabezpieczeniach, które pozwalają przestępcy ominąć uwierzytelnianie operatora kamery i uzyskać bezpośredni dostęp do plików konfiguracyjnych
- Eksploity, które umożliwiają zresetowanie hasła urządzenia, a przez to bezprawną modyfikację plików konfiguracyjnych i dostęp do podstawowych funkcji kamery
- Ataki na kamery, które pozwalają osobom trzecim przechwycić strumienie wideo przesyłane na żywo przez sieć prywatną lub połączenie internetowe

Wiele wymienionych problemów dotyczy licznych mniejszych marek, które korzystają z licencji na technologie dużych dostawców. Oznacza to, że słabe punkty występują w milionach urządzeń. Choć więksi dostawcy o dobrej reputacji często udostępniają poprawki niwelujące problemy, wiele mniejszych firm po prostu je ignoruje. Nawet w przypadku opublikowania poprawki aktualizacje są wprowadzane ręcznie, a właściciele wielu platform monitoringu wideo nie są świadomi zagrożenia. Problem obejmuje też użytkowników domowych, którzy korzystają z różnych systemów monitoringu wideo klasy konsumenckiej. Te kupowane w sklepach detalicznych rozwiązania również często nie są aktualizowane.

Ukierunkowane ataki i botnety

Choć może to się wydawać fabułą hollywoodzkiego hitu, celowe wyłączenie całego systemu monitoringu wideo, który chroni ważne miejsce, obszar czy nawet miasto, nie jest niemożliwe. Wielu dostawców systemów monitoringu wideo korzysta z tych samych bibliotek programowych, które zarządzają takimi elementami jak transmisja strumieniowa, uwierzytelnianie użytkowników czy zapis wideo w pamięci masowej. Dla zręcznych hakerów ataki na monitoring niemal na pewno są więc z jednej strony narzędziem ułatwiającym realizację innych przestępstw, z drugiej – sposobem na wywołanie strachu i paniki.

Kolejną kwestią jest łatwość poruszania się w sieci – przestępcy atakują podłączone do sieci urządzenie, np. kamerę, a potem wykorzystują ten uwierzytelniony element do uzyskania dostępu do innych podłączonych zasobów. Choć dobrze zaprojektowane mechanizmy obronne pozwalają w dużej mierze zablokować takie ataki na sieć, rosnąca powszechność kamer i innych urządzeń Internetu rzeczy (IoT) oraz ich włączenie w podstawowe procesy sprawia, że konieczność zapewnienia urządzeniom IoT dostępu do sieci może zwiększać ryzyko. Ataki na kamery nie są jednak jedynym problemem. Niedawno pojawiły się przypadki, w których przestępcy przejęli same kamery i wykorzystali je jako broń do przeprowadzenia ataków typu „rozproszona odmowa usługi" (DDoS).

Potężny atak DDoS z października 2016 r., który dotknął serwisy Twitter, Amazon, Tumblr, Reddit, Spotify i Netflix, był częściowo wygenerowany przez botnet oparty na szkodliwym oprogramowaniu o nazwie Mirai. Jak mówi specjalistka ds. zabezpieczeń Allison Nixon, szefowa działu badań w firmie Flashpoint, botnet składa się przede wszystkim z urządzeń DVR i kamer IP chińskiego producenta XiongMai Technologies. Komponenty produkowane przez firmę XiongMai są sprzedawane kolejnym dostawcom, którzy wykorzystują je we własnych produktach. Cyberprzestępcy uzyskują tym samym dodatkowo dostęp do dziesiątek tysięcy urządzeń, które mogą wykorzystać w swoich atakach[3].

Administracja publiczna, regulatorzy i przepisy

Gwałtowny wzrost liczby urządzeń podłączonych do Internetu (wg szacunków firm Gartner, Cisco i innych w 2020 r. ma to być 25–50 mld[4]) niepokoi wiele rządów krajowych i regulatorów międzynarodowych. W przeciwieństwie do nadajników radiowych, stacji telewizyjnych czy pojazdów mechanicznych, nie istnieją w zasadzie przepisy, które określałyby, co można podłączyć do Internetu, a co nie. Nie ma wyznaczonych standardów bezpieczeństwa danego elementu. Nie zdefiniowano też, jak postępować, gdy urządzenie zostanie zaatakowane lub wykorzystane do ataku na osobę trzecią. Przepisy karne w większości regionów radzą sobie z cyberprzestępstwami, w których mamy przestępcę i ofiarę. Technologia jest jednak coraz bardziej autonomiczna i pojawia się ryzyko, że niezabezpieczone urządzenia staną się celem wirusów. Epidemie, które nękały użytkowników komputerów, zaczną się wtedy pojawiać na takich urządzeniach jak kamery monitoringu, w przypadku których istnieje mało sposobów na wykrycie lub szybkie wyeliminowanie problemu.

Potencjalna odpowiedzialność finansowa i karna

Nie można też zapomnieć o drażliwej kwestii odpowiedzialności. Instalacja systemów monitoringu wideo może obniżyć koszty ubezpieczenia i zwiększyć prawdopodobieństwo schwytania przestępców. Jeśli jednak system monitoringu wideo stanie się bezużyteczny z powodu ataku na jego zabezpieczenia, a kamery nie zarejestrują popełnionego przestępstwa, firmy ubezpieczeniowe mogą uznać, że nie muszą płacić odszkodowania, ponieważ system monitoringu klienta nie spełniał ustalonych parametrów. Kogo miałaby wtedy pozwać ofiara? Producenta kamery? Dostawcę usług serwisowych dla kamer CCTV? A może – w przypadku incydentu związanego z bezpieczeństwem publicznym – odpowiedzialność ponosiłaby lokalna instytucja państwowa? Naruszenia bezpieczeństwa systemu takiego jak monitoring wideo rodzą wiele pytań, a przypadków testowych jest na tyle mało, że na rynku panuje w tym względzie duża niepewność.

Obawy o ochronę prywatności

Choć kwestia odpowiedzialności finansowej i karnej w związku z atakami hakerów na urządzenia używane do monitoringu wideo wciąż jeszcze jest przedmiotem dyskusji, przepisy o ochronie prywatności obywateli stały się już elementem prawodawstwa większości krajów rozwiniętych. Mogą nieznacznie różnić się w szczegółach, zasadniczo uznaje się jednak, że wszelkie prywatne dane osobowe z takich obszarów jak zdrowie, finanse, orientacja seksualna, poglądy polityczne i wiele innych wymagają gromadzenia i przechowywania w bezpieczny sposób. Dotyczy to również danych wideo. Pacjenci odwiedzający poradnię zdrowia psychicznego czy zwykli ludzie uczestniczący w wiecu politycznym oczekują więc, że wszelkie nagrania z monitoringu wideo będą przechowywane w bezpieczny sposób i niedostępne publicznie. W przypadku cyberataku na urządzenia lub sieci monitoringu wideo istnieje bardzo duże ryzyko, że dane osobowe, takie jak zdjęcia lub inne informacje dotyczące konkretnych osób, zostaną wykradzione i upublicznione bez upoważnienia. Naruszałoby to prawa do ochrony prywatności użytkowników monitorowanych przez system i mogłoby mieć konsekwencje prawne dla podmiotu odpowiedzialnego za przetwarzanie danych osobowych.

Działania administracji publicznej

Administracja krajów na całym świecie dąży do doprecyzowania sposobów ochrony nowej fali urządzeń IoT. W Europie ważni członkowie Komisji Europejskiej otwarcie mówią o procesie certyfikacji dla urządzeń tworzących Internet rzeczy, mającym zapewnić ochronę użytkowników. Komisja pomogła też stworzyć grupę o nazwie Alliance for Internet of Things Innovation, do której należy kilku dużych, czołowych dostawców technologii z sektora energetyki, motoryzacji i ochrony zdrowia. Ma ona rozpocząć prace nad zbiorem zalecanych najlepszych praktyk. Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych opublikował podręcznik ze strategicznymi zasadami ochrony Internetu rzeczy (Strategic Principles for Securing the Internet of Things[5]), w którym poruszono m.in. niektóre kluczowe zagadnienia, takie jak uwzględnianie zabezpieczeń na etapie projektowania, promowanie aktualizowania zabezpieczeń i zarządzanie lukami w zabezpieczeniach w oparciu o ich priorytet wynikający z potencjalnych konsekwencji. Nie ma jednak globalnego ani przyjętego przez całą branżę konsensusu, takiego jak standardy PCI-DSS w sektorze kart kredytowych. W związku z tym bezpieczeństwo urządzeń IoT opiera się obecnie na wytycznych poszczególnych krajów i jest objęte mało rygorystycznymi regulacjami, zróżnicowanymi pod względem zakresu i skuteczności.

Jakie działania podejmuje firma MOBOTIX?

Jako jeden z liderów branży cyfrowego monitoringu wideo firma MOBOTIX wyróżnia się również tym, że całe swoje oprogramowanie opracowuje wewnętrznie. Pozwala to nam oferować bardzo zaawansowane produkty i niesie ze sobą istotne korzyści w dziedzinie bezpieczeństwa. Proces tworzenia oprogramowania jest kontrolowany, w rozwiązaniach MOBOTIX rzadziej pojawiają się więc luki, które mogą zostać wykorzystane do ataku, jak to bywa w przypadku nieodpowiednio zaprojektowanego oprogramowania i sprzętu innych firm. W obszarach, w których korzystamy z powszechnie obsługiwanych standardów branżowych, takich jak ONVIF, dysponujemy politykami przewidującymi udostępnianie wszelkich poprawek niezwłocznie po ich opublikowaniu. We wszystkich modelach kamer MOBOTIX stosowane jest to samo oprogramowanie, nasi międzynarodowi klienci mogą więc łatwiej zadbać o stałą aktualność i bezpieczeństwo oprogramowania wbudowanego.

Od samego początku trzymamy się też koncepcji „security by design", czyli zasady uwzględniania bezpieczeństwa już na etapie projektowania, co przejawia się w wielu aspektach:

Bezpieczny system operacyjny i aktualizacje

MOBOTIX rozpoczyna wprowadzanie zabezpieczeń już na etapie projektowania systemu operacyjnego i aplikacji dla kamery. Wszystkie urządzenia MOBOTIX opierają się na zmodyfikowanym, bezpiecznym systemie operacyjnym Linux, z którego wyeliminowano standardowe usługi i moduły. Inżynierowie z firmy MOBOTIX całkowicie przeprojektowali newralgiczne moduły systemu Linux, takie jak uwierzytelnianie, aby mieć pewność, że nie będą one podatne na standardowe eksploity czy techniki infekowania kodu. Kod źródłowy tego oprogramowania operacyjnego nie jest otwarty, a przy tym chronią go dodatkowe techniki zabezpieczeń. Co więcej, każda aktualizacja oprogramowania wbudowanego urządzenia i aplikacji jest szyfrowana i podpisywana cyfrowo w celu uniknięcia manipulacji.

Bezpieczna konfiguracja kamery

Dostęp do interfejsu konfiguracyjnego kamery mają tylko upoważnieni użytkownicy, a w celu zapewnienia bezpieczeństwa wewnętrznego każdy system umożliwia tworzenie i przypisywanie zróżnicowanych uprawnień różnym grupom użytkowników. W praktyce oznacza to, że kamery MOBOTIX nigdy nie zapisują haseł użytkowników w postaci zwykłego tekstu, lecz przetwarzają je za pomocą silnego, jednokierunkowego algorytmu mieszającego (SHA-512). Nawet gdyby plik konfiguracyjny dostał się w niepowołane ręce, odczytanie faktycznych haseł byłoby niezwykle trudne. Zbędne usługi systemu operacyjnego Linux są wyłączone, aby ograniczyć pole do działania potencjalnych eksploitów i zapobiec atakom. Nie ma tu nieudokumentowanych portów telnet ani „hasła nadrzędnego" – dostęp do kamery MOBOTIX i jej konfiguracja odbywa się przez internetowy graficzny interfejs użytkownika (GUI). Hasła mogą być przechowywane w systemach zarządzania wymagających odpowiednich uprawnień dostępu, takich jak BeyondTrust i CyberArk, które można zabezpieczyć za pomocą skuteczniejszego uwierzytelniania dwuskładnikowego.

Bezpieczna sieć i komunikacja z urządzeniami

Wszystkie dane przesyłane między każdą kamerą MOBOTIX i innymi hostami w sieci mogą być szyfrowane, co pozwala zadbać o ich poufność i integralność. Protokół HTTPS (SSL/TLS) i certyfikaty są obsługiwane w standardzie, co zapewnia zgodność z najlepszymi praktykami zalecanymi dla dużych platform zabezpieczeń przez ekspertów, np. Instytut SANS. Każda kamera MOBOTIX standardowo obsługuje też unikatowe certyfikaty X.509 i certyfikaty głównych jednostek certyfikujących, firmy mogą więc rozszerzyć bezpieczeństwo urządzeń na kamery i wideodomofony uwierzytelniane za pośrednictwem takich systemów jak OpenVPN. Oznacza to, że w przypadku fizycznej kradzieży lub pokonania zabezpieczeń kamery przestępca nie może wykorzystać danych uwierzytelniających w takim urządzeniu do ataku na resztę sieci kamer.

Bezpieczne nagrywanie wewnętrzne i ochrona przed manipulacjami

Wszystkie nagrania wygenerowane przez kamerę mogą zostać zaszyfrowane przed zapisem. Dotyczy to również bufora pierścieniowego, który wykorzystuje wbudowaną w każdą kamerę kartę SD. Firma MOBOTIX stworzyła bezpieczny system plików, w przypadku fizycznej kradzieży lub złamania zabezpieczeń kamery nie można więc pobrać wideo znajdującego się wciąż w urządzeniu bez uzyskania uprawnień administratora, które są chronione przez bezpieczne procesy konfiguracji (opisane wyżej). Każdy obraz wygenerowany przez kamerę MOBOTIX można podpisać cyfrowo za pomocą niestandardowych certyfikatów, aby zapobiec w ten sposób manipulacjom. Dzięki temu nagrania są dopuszczalne jako dowody w sądzie.

Funkcje zabezpieczające	Standardowe kamery IP	MOBOTIX
HTTPS (SSL/TLS) i certyfikaty	✓	✓
Uwierzytelnianie w oparciu o skrót dla HTTP	✓	✓
Listy kontroli dostępu	✓	✓
Indywidualne uprawnienia użytkowników i grup	⚠	✓
Wykrywanie ataków	✗	✓
Ochrona przed botami	✗	✓
Szyfrowanie nagrań	✗	✓
Szyfrowanie wideo i komunikatów	✗	✓
Klient VPN	✗	✓

Wykrywanie ataków

Mimo tak licznych systemów i procesów zabezpieczających lekkomyślnością byłoby założenie, że przestępcy nie będą próbować ataków na kamery MOBOTIX. Dlatego firma inwestuje w dodatkowe narzędzia do wykrywania takich prób. Dzięki wdrożeniu szeregu funkcji do wykrywania ataków każda kamera czy wideodomofon zgłasza za pośrednictwem szyfrowanego kanału wszelkie próby logowania bez autoryzacji i ataki typu brute force. Powiadomienia mogą być też przesyłane w przypadku wielokrotnych nieudanych prób logowania, a adres IP, z którego odbywa się atak, można automatycznie zablokować.

Podsumowanie

Popularność monitoringu wideo – również w służbie zdrowia, sektorze ochrony i procesach przemysłowych – nieprzerwanie rośnie. Systemy tego typu stają się coraz istotniejsze, celami cyberataków coraz częściej będą więc dodatkowe procesy, takie jak kontrola dostępu, monitorowanie środowiska czy procesy analityczne (w tym rozpoznawanie rysów twarzy).

Projektanci systemów monitoringu wideo i usługodawcy, a nawet regulatorzy będą musieli ściślej kontrolować bezpieczeństwo, aby spełnić swoje obowiązki wobec społeczeństwa i wymogi przyszłych przepisów. Liderzy branży, w tym firma MOBOTIX, dostrzegają te kwestie i aktywnie pracują nad włączaniem zabezpieczeń w sprzęt i oprogramowanie urządzeń od najwcześniejszych etapów projektowania.

Skuteczność zabezpieczeń urządzeń jest jednak uzależniona od bezpieczeństwa całego środowiska. Nie ma sensu zamykać drzwi, gdy pozostawiamy otwarte okno. Dlatego projektanci i operatorzy systemów monitoringu wideo i szerszych sieci IoT muszą przyjrzeć się innym częściom środowisk, takim jak sieć bazowa, infrastruktura pamięci masowej, a przede wszystkim personel – ponieważ najsłabszym ogniwem są często ludzie. Kilka organizacji z branży, m.in. Instytut SANS, przygotowało przydatne wskazówki, np. zalecenia Critical Security Controls organizacji Center for Internet Security (CIS). Zawierają one szereg rekomendowanych działań w obszarze cyberbezpieczeństwa, stanowiących konkretne i praktyczne sposoby na powstrzymanie najpowszechniejszych i najbardziej niebezpiecznych ataków[6].

W dalszej perspektywie nie ma wątpliwości, że bezpieczeństwo urządzeń i platform będzie kluczowe w dużych projektach wideo. Wiedza na temat wyzwań związanych z IoT staje się coraz powszechniejsza, MOBOTIX liczy więc na wspólną pracę z innymi firmami z branży, klientami i organami administracji publicznej nad ochroną technologii i systemów, które zwiększają bezpieczeństwo całego społeczeństwa.

Materiały referencyjne

https://www.coresecurity.com/system/files/publications/2016/05/corelabs-ipcams-research-falcon-riva.pdf

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Źródła

[1]https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.

[2]html https://www.coresecurity.com/advisories/hikvision-ip-cameras-multiple-vulnerabilities

[3]https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

[4]http://www.telecomtv.com/articles/iot/internet-of-things-to-reach-25-billion-devices-within-five-years-11931/

[5]https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[6]https://uk.sans.org/critical-security-controls

Firma MOBOTIX od 2000 r. opracowuje i produkuje w Niemczech systemy wideo IP oraz oprogramowanie do zarządzania plikami wideo i ich analizy.

Produkty MOBOTIX wyróżniają się **wysokim stopniem niezawodności**. Wszystkie kamery zewnętrzne poddawane są testom obciążeniowym w temperaturach od -30°C do +60°C (od -22°F do +140°F). Urządzenia działają bez dodatkowych elementów, systemów ogrzewania i chłodzenia, nie mają też części ruchomych (na przykład automatycznej przesłony), nie wymagają więc niemal konserwacji.

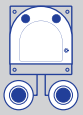
MOBOTIX oferuje **pakiet znakomicie dopasowanych rozwiązań** – od karty microSD do zapisywania danych i systemu audio HD (mikrofon i głośnik) z telefonią VoIP, przez analizę wideo i profesjonalny system do zarządzania obrazem wizyjnym, po oprogramowanie do wykrywania ruchu, które ogranicza fałszywe alarmy.

Zdecentralizowana architektura oznacza, że nie jest tu wymagany komputer centralny, a obciążenie dla sieci jest minimalne. Inteligentne kamery MOBOTIX same przetwarzają i przechowują obrazy oraz aktywują zdarzenia, a w przypadku dostępu zdalnego dostosowują liczbę klatek na sekundę i rozdzielczość do przepustowości łącza.

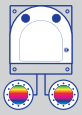
Dzięki nowym **czujnikom 6MP Moonlight** i uzupełniającej je **technologii obrazowania termowizyjnego** możliwe jest niezawodne wykrywanie poruszających się obiektów, nawet w najtrudniejszych warunkach oświetleniowych i na duże odległości. Dzięki temu można zabezpieczać rozległe obszary za pomocą zaledwie kilku kamer. Zmniejsza to również zapotrzebowanie na okablowanie zasilające, infrastrukturę IT i dodatkowe źródła światła. Kamery MOBOTIX są zasilane w standardowej technologii PoE i nie wymagają mocy większej niż 4–5 W.

Inteligentny system wideo IP firmy MOBOTIX pozwala na **zmniejszenie łącznych kosztów**. Wydane pieniądze po krótkim czasie zaczynają się zwracać, a dzięki dołączanemu bez dodatkowych opłat oprogramowaniu i jego aktualizacjom inwestycja jest po prostu przyszłościowa.

Zewnętrzne dwuobiektywowe

M16 AllroundDual	S16 FlexMount	D16 DualDome
		
Wytrzymałość w ekstremalnych warunkach	Elastyczna kamera dwuobiektywowa	Modułowa kamera dwuobiektywowa

Termowizyjne

M16 Thermal	S16 DualThermal
	
Dwuobiektywowa kamera termowizyjna	Dwuobiektywowa kamera termowizyjna

Zewnętrzne jednoobiektywowe

M26 Allround	S26 FlexMount	Q26 Hemispheric	D26 Dome
			
Wytrzymałość w ekstremalnych warunkach	Dyskretny wygląd, analiza wideo	Dyskretny wygląd, analiza wideo	Modułowa kamera kopułkowa

Kamery wewnętrzne

i26 Panorama	c26 Hemispheric	p26 Allround	v26 MiniDome
			
Hemisferyczna kamera 180°	Dyskretny wygląd, analiza wideo	Modułowa kamera sufitowa	Kamera wandaloodporna

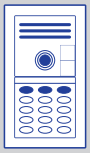
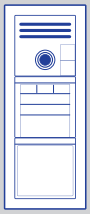
Moduły wideodomofonu

Kamera	BellRFID	Klawiatura
		

MxDisplay+

Stacja zdalna


Zestawy drzwiowe

Ramka podwójna		Ramka potrójna	
			

PL_11/17

MOBOTIX AG
Kaiserstrasse
D-67722 Langmeil, Niemcy
Tel.: +49 6302 9816-103
Faks: +49 6302 9816-190
sales@mobotix.com
www.mobotix.com

MOBOTIX