**Kamery CCTV to ulubiony sposób dostępu cyberprzestępców do sieci firmowych!**

**Kamery bezpieczeństwa podłączone do Internetu są obecnie wszędzie – w miejscach publicznych, organizacjach, a nawet w prywatnych domach. Ich rynek był w 2021 roku warty około 50 miliardów dolarów, a ma przed sobą perspektywę dalszego wzrostu. Każdego dnia na całym świecie instaluje się i łączy setki tysięcy kamer bezpieczeństwa. Jak jednak wygląda kwestia ich własnego bezpieczeństwa?**

Kamery CCTV są szybko opracowywane przez producentów. Bardziej zaawansowane wersje wyposażone w inteligentne czujniki i zaawansowane oprogramowanie oferujące funkcje takie jak noktowizor, wykrywanie odległości, wykrywanie ciepła i ruchu. Na drugim końcu znajdują się mniej zaawansowane kamery domowe, którymi można zarządzać za pomocą aplikacji na smartfony.

Jak twierdzi Miri Ofir, dyrektor działu R&D w Check Point Software, obecnie CCTV (lub kamery bezpieczeństwa podłączone do Internetu) są jednym z ulubionych sposobów penetracji sieci korporacyjnych przez cyberprzestępców, ponieważ są z natury podatne na ataki i służą jako najłatwiejszy punkt wejścia dla atakujących!

Jakie informacje mogą uzyskać atakujący za pomocą tych kamer? Kamery bezpieczeństwa, których obecnie używamy w wielu organizacjach, to zaawansowane urządzenia, wyposażone w możliwości przetwarzania obrazu i dźwięku. Ich systemy nagrywania oferują możliwości dekodowania tekstu i rozpoznawania twarzy. Informacje z tych kamer są przesyłane do chmury w celach telemetrycznych lub w celu uzyskania wartości z możliwości analitycznych zapewnianych przez usługi AI.

- *Poufne dane, które przechodzą przez kamery bezpieczeństwa, mogą narazić operatorów na różne problemy związane z prywatnością i budzą poważne obawy dotyczące możliwości podglądania lub podsłuchiwania poufnych informacji. W Stanach Zjednoczonych wydano dyrektywę zakazującą używania niektórych kamer bezpieczeństwa we wszystkich siedzibach agencji federalnych. Dyrektywa wymagała demontażu i wymiany istniejącego sprzętu ­­*– zauważa ekspert Check Pointa. Podobne głosy słychać również w kilku krajach europejskich, ponieważ pojawiły się przykłady, w których niektóre kamery mogą działać jako aktywny lub uśpiony środek, używany do woli.

Atakujący wiedzą, że kamery oraz urządzenia nagrywające zawierają poufne informacje, które we właściwych rękach mogą być bardzo dochodowe, co czyni je ogromnym celem.

**Dlaczego tak trudno jest zabezpieczać kamery bezpieczeństwa?**

Kamery bezpieczeństwa są połączone zarówno z siecią firmową, jak i z Internetem, przechwytując i przesyłając duże ilości danych do systemów rejestrujących znajdujących się w organizacji lub w chmurze. System zarządzania kamerą może być tworzony i zarządzany wewnętrznie lub zarządzany za pośrednictwem strony internetowej producenta urządzenia. Urządzenia nagrywające (DVR/NVR) przetwarzają wideo, tworząc pliki kopii zapasowych, które można zapisywać na firmowych serwerach pamięci masowej (NAS) przez różne okresy, zgodnie z polityką firmy.

Powszechną praktyką bezpieczeństwa, jest separacja sieci dla podłączonych urządzeń IoT (lub przynajmniej wdrożenie segmentacji w obrębie sieci). Jednak realizacja jest niezwykle trudna dla administratorów sieci. Często, ich zdaniem, czas potrzebny na ręczne wdrożenie przeważa nad efektem końcowym. Ponadto takie postępowanie wiąże się z wysokimi kosztami w fazie zakładania i eksploatacji.

Innym powodem, dla którego te urządzenia są tak trudne do zabezpieczenia, jest to, że większość urządzeń IoT jest domyślnie instalowana z oprogramowaniem układowym producenta, które nierzadko posiada luki w oprogramowaniu pochodzące z błędów lub słabej inżynierii oprogramowania. Co więcej, naprawa lub aktualizacja oprogramowania zawsze wymaga aktualizacji kodu. Producenci urządzeń IoT w żadnym wypadku nie są ekspertami w dziedzinie bezpieczeństwa i wielu z nich woli dostarczać nieobciążające oprogramowanie, pomijając kluczowe zasady pisania zabezpieczonego kodu.

Producenci zazwyczaj używają pakietów open-source i standardowych komponentów innych firm, które mogą narazić urządzenie na znane problemy. Open-source jest ogromną zaletą dla programistów, ale wymaga częstych aktualizacji za każdym razem, gdy publikowana jest luka w oprogramowaniu. Niestety, producenci IoT niekoniecznie zapewniają tworzenie poprawek bezpieczeństwa dla swoich urządzeń. - *Prawda jest taka, że świadomość bezpieczeństwa jest niewystarczająca, a zapotrzebowanie użytkowników na bezpieczeństwo w ramach tych urządzeń nie jest wystarczająco silne. Nawet w scenariuszach, w których producenci biorą odpowiedzialność za bezpieczeństwo swoich urządzeń i wydają okresowe aktualizacje zabezpieczeń, wielu ich klientów rzadko zadaje sobie trud aktualizowania swoich urządzeń* – zauważa Miri Ofir.

Jest wiele powodów, dla których tak się dzieje. Pierwszy powód ma związek z wydajnością operacyjną i wysiłkiem wymaganym do utrzymania systemów rozproszonych. W wielu przypadkach aktualizacja oprogramowania sprzętowego na urządzeniu IoT jest bardziej skomplikowana niż aktualizacja oprogramowania na komputerze osobistym. Nadal istnieją urządzenia, które polegają na aktualizacjach jedynie przez USB! Co więcej, zdarzają się przypadki, w których urządzenia są instalowane w niedostępnych miejscach (np. kamery zainstalowane na ogrodzeniach, wysokich słupach lub setki kilometrów od kadry zarządzającej). Ponadto aktualizacje oprogramowania wymagają ponownego uruchomienia urządzeń, co może być problematyczne lub bardzo wrażliwe ze względu na krytyczne funkcje urządzenia.

Na końcu warto zwrócić uwagę na złośliwe aktualizacje. - *Istnieje wiele przykładów ataków pochodzących z aktualizacji oprogramowania, takich jak słynny atak na łańcuch dostaw, który widzieliśmy za pośrednictwem aktualizacji SolarWinds* – mówi dyrektor w firmie Check Point Software.

**Jak atakujący wykorzystują luki w oprogramowaniu?**

Hakerzy często wybierają ścieżkę najmniejszego oporu. Każda znana luka (CVE) staje się potencjalną bronią dla cyberprzestępców, którzy mogą przeniknąć do organizacji. Luki zwykle wykrywane po tym, gdy zostaną ujawnione przez atakujących, a szkody zostaną już wyrządzone. W najlepszym przypadku badaczom podatności udaje się zidentyfikować słabe punkty w środowisku laboratoryjnym w ramach projektu badawczego lub artykułu. Następnie dają producentom 90-dniowy okres na wydanie aktualizacji oprogramowania przed opublikowaniem informacji o luce. - *To dla producentów często zbyt mało czasu – co oznacza, że muszą przerwać to, nad czym obecnie pracują, i wydać szybkie aktualizacje, zanim luka zostanie opublikowana ­­*– mówi Ofir.

Najpoważniejsze CVE odnoszą się do możliwości zdalnego uruchamiania kodu (RCE - Remote Code Execution). Ten rodzaj ataku umożliwia pełną kontrolę nad urządzeniem z dowolnej zdalnej lokalizacji oraz kradzież informacji, uruchamianie oprogramowania ransomware, instalowanie koparek walut cyfrowych na urządzeniu, umieszczanie bota w celu umożliwienia wykonywania dodatkowych działań itd. Atakując urządzenie podłączone do sieci firmowej, sprytni napastnicy uzyskują możliwość dotarcia do dowolnego komputera w sieci i uruchomienia zdalnych poleceń. Widzimy, jak ta metoda staje się coraz bardziej wyrafinowana w miarę upływu czasu. Atakujący penetrują nawet organizacje i decydują się czasem pozostać „uśpionym” przez wiele miesięcy, dopóki nie zdecydują, że jest właściwy moment na uderzenie.

**Jak zapewnić bezpieczeństwo?**

*- Istnieje kilka sposobów na zminimalizowanie zagrożeń cybernetycznych pochodzących z urządzeń IoT. Urządzenia można podzielić na różne kategorie, przy czym każda kategoria otrzymuje inny poziom ryzyka. Na szczycie listy znajdują się urządzenia z „oczami i uszami”, takie jak kamery, windy, drony, a nawet routery. Najlepszą praktyką jest zakup urządzeń od uznanej, sprawdzonej i rzetelnej firmy. Wdrożenie powinno być ściśle zaplanowane, w tym bieżące monitorowanie, identyfikacja anomalii oraz formułowanie procedur aktualizacji dla tych urządzeń* – wyjaśnia ekspert cyberbezpieczeństwa.

Na rynku są rozwiązania (np. Quantum IoT Protect), które pozwalają producentom zapewnić bezpieczeństwo swoich kamer czy innych urządzeń IoT. Dlatego konsumenci powinni wybierać producentów, którzy chcą inwestować we wbudowane zabezpieczenia. Monitorowanie już nie wystarcza. Wykrycie ataku, który już nastąpił, jest niewystarczające, bo szkoda najprawdopodobniej jest już wyrządzona.

ć