INNERGO.

BEZPIECZEŃSTWO SYSTEMÓW WIDEOKONFERENCYJNYCH

W ostatnim czasie, wśród przedsiębiorstw, zaobserwować mogliśmy znaczny wzrost zainteresowania narzędziami do pracy zdalnej, w tym szeroko pojętymi systemami wideokonferencyjnymi. Niestety, zwróciło to także uwagę środowisk hakerskich, dlatego należy bacznie przyjrzeć się obecnie wykorzystywanym narzędziom pracy pod kątem ich bezpieczeństwa.Szczególnie podatne na ataki są systemy i urządzenia starszej generacji. W związku z tym nie tylko odpowiednia konfiguracja, ale także aktualizacja posiadanych systemów i narzędzi może zabezpieczyć przed konsekwencjami ataku hakerskiego.

Na co zwrócić szczególną uwagę?

Z punktu widzenia bezpieczeństwa należy przede wszystkim zwrócić uwagę na rozwiązania wykorzystujące protokół H.323. Wielu producentów zrezygnowało już z jego wspierania, przez co stało się bardziej podatnymi na ataki. Do zaatakowania terminala bazującego na protokole H.323 nierzadko wystarczy odpowiednio spreparowany pakiet inicjalizujący sesję tzw. H.323 SETUP, wysyłany na wcześniej zeskanowany przez hakerów adres IP i port TPC 1720.

Należy jednak podkreślić, iż różnego odzaju podatności systemów konferencyjnych mogą skutkować różnymi zagrożeniami: od zablokowania systemu, przez jego przejęcie i generowanie dodatkowych kosztów, kończąc na możliwości podsłuchiwania i podglądania uczestników, jak również dyskretnego monitorowania tego, co dzieje się na samych salach konferencyjnych. Zamiast protokołu H.323 producenci postanowili rozwijać protokół SIP, który obecnie jest najczęściej wykorzystywany w rozwiązaniach wideo i audio konferencyjnych. Dzięki szerokiemu rozpowszechnieniu i wieloletniemu rozwijaniu, protokół SIP jest obecnie najszerzej wykorzystywanym protokołem komunikacyjnym w środowiskach konferencyjnych, ale także w telefonii stacjonarnej (szerzej znanej jako VoIP – Voice over IP).

Jakie są sposoby zabezpieczeń?

W celu zabezpieczenia narzędzi telekomunikacyjnych producenci oferują coraz to nowsze rozwiązania technologiczne. Wśród istotnych rozwiązań bezpieczeństwa, które warto wdrożyć u siebie, można wyróżnić m.in.:

- Nowoczesne, dedykowane do systemów telekomunikacyjnych i konferencyjnych rozwiązania brzegowe. Specjalne systemy, których celem jest wsparcie firewalli – działających na styku z internetem – o dodatkową obsługę skomplikowanych protokołów telekomunikacyjnych, a nierzadko także dostosowanie różnych parametrów czy kodowania pomiędzy stronami komunikacji.

- Szyfrowanie protokołów komunikacyjnych tzw. Secure SIP. SIPS jest jednym z tych narzędzi, dzięki którym atak hakerów może zostać udaremniony.

- Szyfrowanie rozmów z wykorzystaniem protokołu SRTP. Dzięki możliwości szyfrowania strumieni multimedialnych (głosu, wideo, czy prezentacji) mamy pewność, że osoba postronna nie będzie w stanie przechwycić strumienia i podsłuchiwać prowadzonych komunikacji.

Od czego zacząć zabezpieczanie swoich rozwiązań telekomunikacyjnych?

1 Przeprowadzić audyt rozwiązania wideokonferencyjnego jak i telekomunikacyjnego. Sprawdzenie wykorzystywanych protokołów, wersji urządzeń oraz używanych zabezpieczeń jest podstawowym krokiem do rozpoczęcia zabezpieczania rozwiązania.

2 Opracowanie kompleksowego planu zabezpieczenia infrastruktury. Bazując na zdobytej w czasie audytu wiedzy możliwe jest zbudowanie planu zabezpieczenia i rozwoju rozwiązań konferencyjnych i telekomunikacyjnych. Możliwe jest zarysowanie szybkich, krótkofalowych celów, jak również rozwój w szerszej perspektywie czasu.

3 **Wdrożenie opracowanego planu zabezpieczenia rozwiązania.**

A) Najczęstszym środkiem doraźnym jest aktualizacja wersji oprogramowania. Częstym zaniedbaniem jest bazowanie na nieaktualnych wersjach oprogramowania, przez co urządzenia jak i aplikacje mogą być łatwym celem dla hakerów.

B) W wielu przypadkach już posiadane rozwiązania sprzętowe mogą być poza wsparciem producenta, przez co są podatne na ataki. W takim wypadku nierzadko niezbędna jest wymiana na nowe rozwiązanie.

C) Wdrożenie dodatkowych zabezpieczeń zgodnie z opracowanym planem.

4 Stałe utrzymanie bezpieczeństwa systemów. Poprzez utrzymywanie odpowiednich poziomów wsparcia technicznego, INNERGO może dostarczać wszelkich uaktualnień niedługo po wykryciu przez producentów luk w bezpieczeństwie i stabilności swoich rozwiązań. Ponadto stała opieka serwisowa umożliwia także proaktywne działania i rozwój posiadanej infrastruktury.

SKONTAKTUJ SIĘ Z NAMI

biuro@innergo.pl

22 87 37 700