

Cyberprzestępcy wykorzystują wizerunek Urzędu Ochrony Danych Osobowych (UODO) do wyłudzenia szczegółowych informacji o systemach monitoringu wizyjnego. Do przedsiębiorstw zajmujących się instalacją kamer trafiają fałszywe wiadomości e-mail, które wyglądają jak oficjalna korespondencja urzędowa. Oszuści żądają danych umożliwiających identyfikację urządzeń, ich lokalizacji oraz użytkowników. UODO ostrzega, że nie wysyłał takich wezwań, a przekazanie informacji może stworzyć poważne zagrożenie dla bezpieczeństwa osób i mienia.

Fałszywe wezwania trafiają do firm

19 października 2026 roku zespół CSIRT GOV poinformował UODO o kampanii phishingowej skierowanej do przedsiębiorstw instalujących monitoring wizyjny.

W rozsyłanych wiadomościach przestępcy powołują się na rzekomą analizę zgodności systemów monitoringu z przepisami RODO. Przywołują konkretne artykuły unijnego rozporządzenia dotyczące bezpieczeństwa danych oraz obowiązków administratorów.

Wiarygodność korespondencji mają zwiększać dane teleadresowe przypominające rzeczywiste informacje o urzędzie, formalny język oraz załączona tabela do wypełnienia.

Adresaci otrzymują żądanie przekazania zestawienia instalacji wykonanych w ciągu ostatnich 12 miesięcy. Na odpowiedź wyznaczono siedem dni roboczych, a dokument przedstawiono jako urzędowe wezwanie.

Jakich informacji żądają przestępcy?

Fałszywa korespondencja zawiera prośbę o przekazanie szczegółowych danych technicznych i lokalizacyjnych.

Wśród wymaganych informacji znajdują się dane kontaktowe użytkowników końcowych, dokładne lokalizacje kamer wraz ze współrzędnymi geograficznymi, adresy IP urządzeń, numery seryjne, modele oraz wersje zainstalowanego oprogramowania.

Tak przygotowane zestawienie mogłoby ujawnić nie tylko miejsca funkcjonowania systemów monitoringu, ale również ich potencjalne słabości techniczne.

Szczególnie niebezpieczne jest przekazanie informacji o wersjach oprogramowania, ponieważ mogą one pomóc w identyfikacji urządzeń korzystających z nieaktualnych zabezpieczeń.

Zagrożenie dla bezpieczeństwa osób i mienia

Pozyskanie danych technicznych kamer może stanowić pierwszy etap bardziej zaawansowanego cyberataku.

Przestępcy mogą próbować wykorzystać znane podatności oprogramowania lub niezmienione ustawienia fabryczne urządzeń. W określonych przypadkach może to prowadzić do uzyskania nieuprawnionego dostępu do systemu monitoringu.

Oszuści podszywają się pod UODO. Uwaga na fałszywe wezwania

Kategoria: Aktualności

Opublikowano: środa, 21, październik 2026 08:18

Tomasz Smaś

Odśloni: 259

Przejęcie kontroli nad kamerami stwarza ryzyko podglądu obrazu, naruszenia prywatności oraz ujawnienia informacji o zabezpieczeniach budynków i obiektów. Zagrożenie dotyczy zarówno przedsiębiorstw, jak i instytucji oraz osób korzystających z monitoringu wizyjnego.

UODO zaprzecza wysyłaniu takich pism

Urząd Ochrony Danych Osobowych jednoznacznie wskazuje, że nie jest nadawcą opisanej korespondencji.

UODO nie rozsyła tego rodzaju ankiet ani urzędowych wezwań do sporządzania szczegółowych wykazów instalacji monitoringu. Nie prowadzi również zbierania informacji w formie przedstawionej przez oszustów.

Opisane działania stanowią przykład phishingu, czyli oszustwa polegającego na podszywaniu się pod zaufane instytucje w celu pozyskania poufnych danych.

Jak chronić się przed oszustwem?

Podstawową zasadą bezpieczeństwa pozostaje weryfikowanie autentyczności otrzymywanej korespondencji, szczególnie gdy zawiera żądanie przekazania szczegółowych informacji technicznych.

Nie należy uznawać wiadomości za wiarygodną wyłącznie dlatego, że zawiera nazwę urzędu, odwołania do przepisów lub formalnie sformułowane wezwanie. W przypadku wątpliwości konieczne jest sprawdzenie nadawcy i potwierdzenie autentyczności pisma za pomocą oficjalnych kanałów kontaktu z instytucją.

Ostrzeżenie UODO pokazuje, że cyberprzestępcy coraz częściej wykorzystują pozory urzędowych procedur do zdobywania informacji mogących posłużyć do kolejnych ataków. Zachowanie ostrożności przy udostępnianiu danych o monitoringu ma zatem bezpośrednie znaczenie dla bezpieczeństwa cyfrowego i fizycznego.

Źródło: UODO