

UNCUT- NEWS

NIEZALEŻNE ANALIZY I INFORMACJE NA TEMAT GEOPOLITYKI, EKONOMII, ZDROWIA, TECHNOLOGII



Wielki Brat jest wbudowany bezpośrednio w ekran

- [13 października 2025 r.](#)

Nawet w trybie czuwania telewizory nadal sygnalizują chęć skorzystania z usługi. Oto, co możesz z tym zrobić.

Autorka: Christiny Maas

Kiedy europejscy regulatorzy zaczęli przyglądać się eleganckim, czarnym ramkom nowoczesnych telewizorów, nie spodziewali się, że w tle dyskretnie będzie działać niewielka organizacja inwigilacyjna.

Właśnie to odkryli: telewizory, które zachowywały się mniej niż pasywne ekrany, a bardziej jako cyfrowi donosiciele – z bezpośrednim połączeniem do międzynarodowej sieci sprzedawców danych, dostawców oprogramowania, serwisów streamingowych i każdego, kto byłby skłonny zapłacić za kawałek twojego salonu.

Okazuje się, że jedyną rzeczą, która jest naprawdę „włączona” w telewizorach typu smart TV, jest założenie, że wyłączenie telewizora cokolwiek da.

Śledztwo

Dochodzenie zostało wszczęte w ramach wspólnego projektu RODO przez organy ochrony danych z Holandii, Węgier, Włoch i Liechtensteinu.

Wybrali trzy najlepiej sprzedające się telewizory Smart TV na rynku europejskim. Mniej testowano sam produkt, bardziej tajne operacje.

Rejestrowano surowy ruch sieciowy w normalnych warunkach: podczas konfiguracji, w stanie bezczynności, po 24 godzinach od wyłączenia urządzenia i podczas normalnego użytkowania.

Efekt: Twój telewizor jest zaskakująco zajęty, jak na zestaw, który powinien wyświetlać wyłącznie powtórki programu „Bake Off”.

Podczas instalacji ponad 96% danych wychodzących w jednym modelu trafiło bezpośrednio do dostawcy systemu operacyjnego.

Inne urządzenie wysłało jedną trzecią swojego początkowego ruchu do serwisów streamingowych. Producenci – których nazwy widnieją na pudełku – ledwo pojawili się w strumieniu danych.

Domeny osób trzecich podsłuchiwały jeszcze przed wyjęciem pilota z plastikowego opakowania.

I na tym się nie kończy. Nawet po wyłączeniu telewizora.

„Uznaliśmy za interesujące, że nawet po wyłączeniu urządzenia nadal istnieją połączenia z serwisami streamingowymi, producentem i innymi podmiotami zewnętrznymi” – czytamy w raporcie – w tonie, który sugeruje, że autorzy chcieliby krzyczeć.

Jedno urządzenie przekierowało ponad 98% ruchu w trybie gotowości do dostawcy systemu operacyjnego.

Co jest przekazywane

Dane przesyłane przez te urządzenia można porównać do menu bufetu, w którym można śledzić wszystko:

- Prywatne adresy IP
- Identyfikatory urządzeń
- Identyfikatory kont
- Identyfikatory reklamowe
- Wersje oprogramowania sprzętowego
- Ustawienia
- Dzienniki użytkowania
- Znak czasu

Dokładnie tego nie chcesz po cichu przesyłać do sieci zewnętrznej podczas oglądania serialu.

Wszystko to wspiera model biznesowy, który ma mniej wspólnego z budową telewizorów, a więcej ze sprzedażą tych, którzy je oglądają.

Producenci uciekają

W raporcie stwierdzono: „Konsument (osoba, której dane dotyczą) ma do czynienia z wieloma firmami lub podmiotami podczas korzystania ze swojego telewizora Smart TV. Wszyscy objęci badaniem producenci współpracują z partnerami”.

Ten przyjazny język maskuje cyniczną maszynę do zarabiania pieniędzy, w której producenci zawierają umowy, instalują aplikacje fabrycznie, wymuszają treści i czerpią zyski z każdej sekundy oglądania.

W niektórych przypadkach aplikacji tych nie można było usunąć. W innych instalowały się automatycznie, bez powiadomienia użytkownika. Dane osobowe były udostępniane nawet bez konieczności zakładania konta u dostawcy.

Zgodnie z RODO, administrator danych ponosi faktyczną odpowiedzialność. Producenci zachowują się jednak tak, jakby byli jedynie dalekimi kuzynami Twoich danych, a nie tymi, którzy zainstalowali oprogramowanie szpiegujące.

Wielu przerzuca odpowiedzialność na dostawców systemów operacyjnych lub twórców aplikacji. Niektórzy niechętnie podpisują umowy o przetwarzaniu danych. Te jednak zapewniają niewielką przejrzystość.

Efektem końcowym jest nieprzejrzysty system, w którym użytkownicy są zmuszani do akceptowania skomplikowanych warunków korzystania od wielu stron – aby w ogóle móc oglądać telewizję.

„We wszystkich markach użytkownicy spotykają się z sytuacjami, w których nie mają innego wyjścia, jak zaakceptować kompleksową politykę prywatności, aby móc korzystać z urządzenia” – czytamy w raporcie.

Oglądać telewizję? Tylko jeśli rezygnujesz ze swojej prywatności.

Fragmentaryczny nadzór

Wszyscy badani producenci mają siedzibę poza EOG. Oznacza to, że nie ma jednolitego nadzoru w ramach RODO.

Każda władza krajowa musi działać indywidualnie – z „lokalnym zaangażowaniem” przeciwko międzynarodowej hydrze.

Co możesz z tym zrobić?

Oto kroki, aby ograniczyć wbudowane urządzenie monitorujące w salonie. Nie da się tego całkowicie wyeliminować – telewizory Smart TV są zaprojektowane tak, aby podsłuchiwać nawet wtedy, gdy powiesz „stop”. Możesz jednak powstrzymać napływ danych:

1. Wyłącz śledzenie i telemetrię

Przejdź do Ustawienia → Prywatność / Reklama / Ogólne / Pomoc.

Wyłącz opcje takie jak:

- „Przeglądanie informacji”
- „Reklama oparta na zainteresowaniach”
- „Żyj Plus”
- „Promocja domu”
- „Doświadczenie Smart TV”
- „Ogranicz śledzenie reklam”

Przykłady:

- Samsung: Wyłącz „Usługi przeglądania informacji” i „Reklamy oparte na zainteresowaniach”.
- LG: Wyłącz opcję „Live Plus”, wyłącz opcję „Home Promotion” i włącz opcję „Limit Ad Tracking”.

Wyłącz także raporty diagnostyczne i raporty użytkowania.

2. Wyłącz kamerę i mikrofon

- Cofnij uprawnienia dostępu („Usługi głosowe”, „Dostęp do mikrofonu”).
- Jeśli to możliwe, należy używać przełączników fizycznych.
- Zakryj lub odsuń kamerę.
- Wyłącz opcję „Zawsze nasłuchuj” i sterowanie głosowe.

3. Nie zakładaj konta producenta

Pomiń rejestrację w przypadku kont marek (Samsung, LG).

Unikaj dodatkowych uprawnień w aplikacjach (np. dotyczących lokalizacji).

4. Rozłącz się z Internetem

Brak internetu = brak transferu danych.

- Wyłącz Wi-Fi lub odłącz kabel LAN, jeśli nie jest potrzebny.
- Użyj trybu offline, aktualizacje przeprowadzaj ręcznie przez USB.

Wada: funkcje strumieniowe i inteligentne nie będą działać.

5. Skonfiguruj bloki sieciowe

Blokuj śledzenie na poziomie routera:

- **Pi-hole** do blokowania DNS
- Reguły zapory dla określonych adresów IP

- Sieć gościnna dla telewizji z minimalnymi uprawnieniami
- Router z filtrem domenowym

Dzięki temu masz centralną kontrolę.

6. VPN na poziomie routera

Kieruj ruch telewizyjny przez VPN.
Ukrywa to adres IP i lokalizację.

Ale: niektóre serwisy streamingowe blokują sieci VPN, a ich konfiguracja może być problematyczna.

7. Monitoruj ruch danych

- Sprawdź logi routera, zablokuj nowe domeny.
- Należy zachować ostrożność w przypadku usług systemowych (np. aktualizacji).
- Pomyśl o „cyfrowym zwalczaniu szkodników” – ciągłym i pracochłonnym, ale koniecznym.

8. Całkowicie zrezygnuj z funkcji inteligentnych

Najbardziej radykalne rozwiązanie: **kupić „głupi” telewizor** bez internetu.
Użyj urządzeń do streamingu lub zewnętrznych głośników, którymi łatwiej sterować.

Dzięki temu telewizor znów staje się czystym wyświetlaczem, a nie źródłem informacji o tobie.

Wniosek

Wyłączenie śledzenia skutkuje utratą wygody – sterowanie głosowe, personalizacja i rekomendacje nie są już dostępne.

Niektórym zbieraniu danych można zapobiec jedynie wtedy, gdy urządzenie jest całkowicie offline.

A producenci regularnie zmieniają metody śledzenia – użytkownicy muszą stale nadążać.

Oznacza to, że każdy, kto dziś kupi inteligentny telewizor, nie tylko otrzyma wyświetlacz do swojego salonu, ale także stały kanał przesyłu własnych danych do firm zewnętrznych.

[Źródło: Big Brother Comes Built Into the Screen](#)