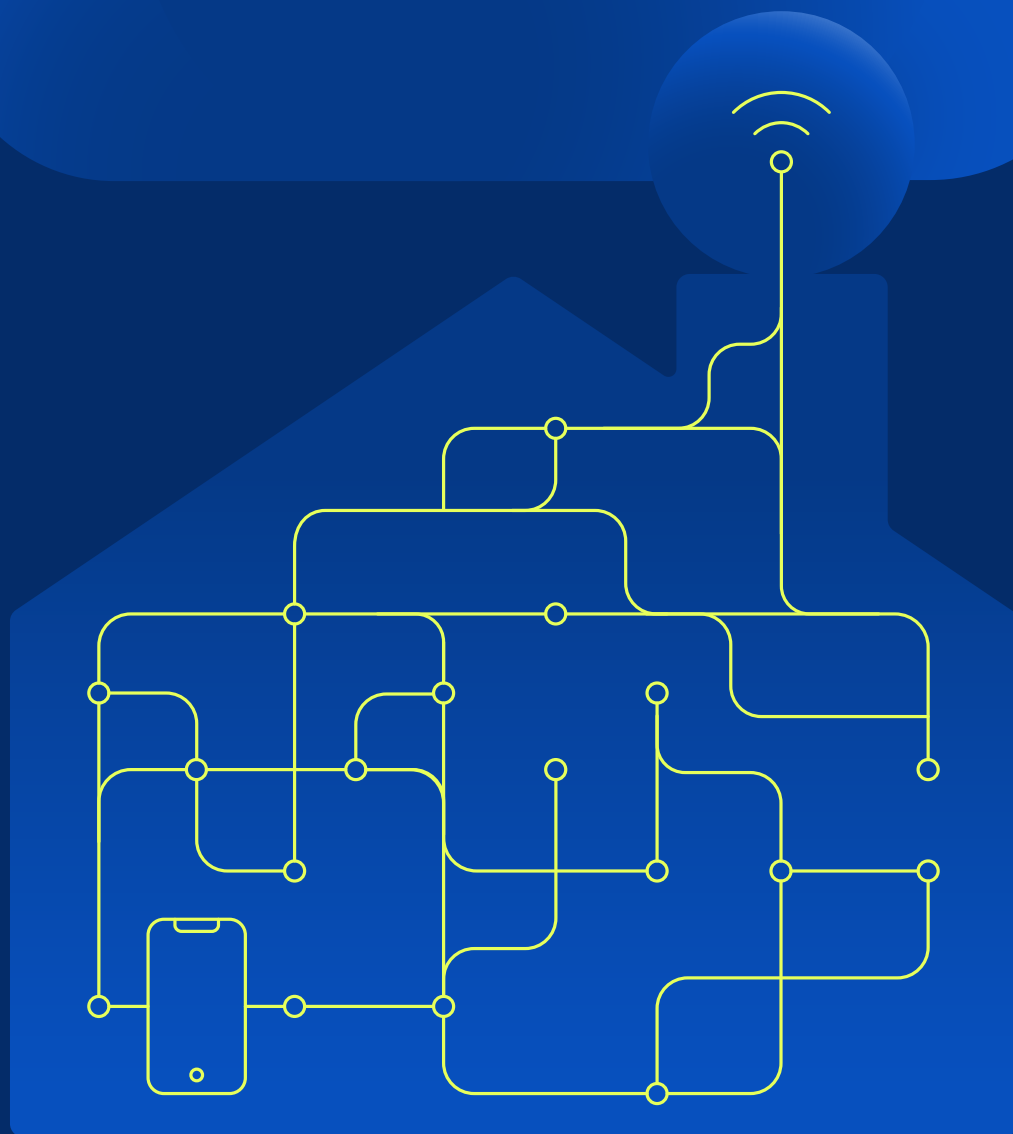


Urządzenia IoT w domu

Jak korzystać z nich bezpiecznie?



NASK

TYTUŁ

Urządzenia IoT w domu. Jak korzystać z nich bezpiecznie?

AUTORZY

Katarzyna Grabowska, Anna Felkner

WSPARCIE MERYTORYCZNE

Karol Bojke

REDAKCJA JĘZYKOWA I KOREKTA

Katarzyna Nakonieczna, Łukasz Szczęsny

PROJEKT GRAFICZNY

NASK – PIB

Publikacja jest rozpowszechniana na zasadach licencji Creative Commons.
Uznanie autorstwa – Użycie niekomercyjne (CC BY-NC) 4.0 Międzynarodowe.

ISBN 78-83-68356-62-5

2026

NASK – Państwowy Instytut Badawczy
ul. Kolska 12, 01-045 Warszawa

www.nask.pl

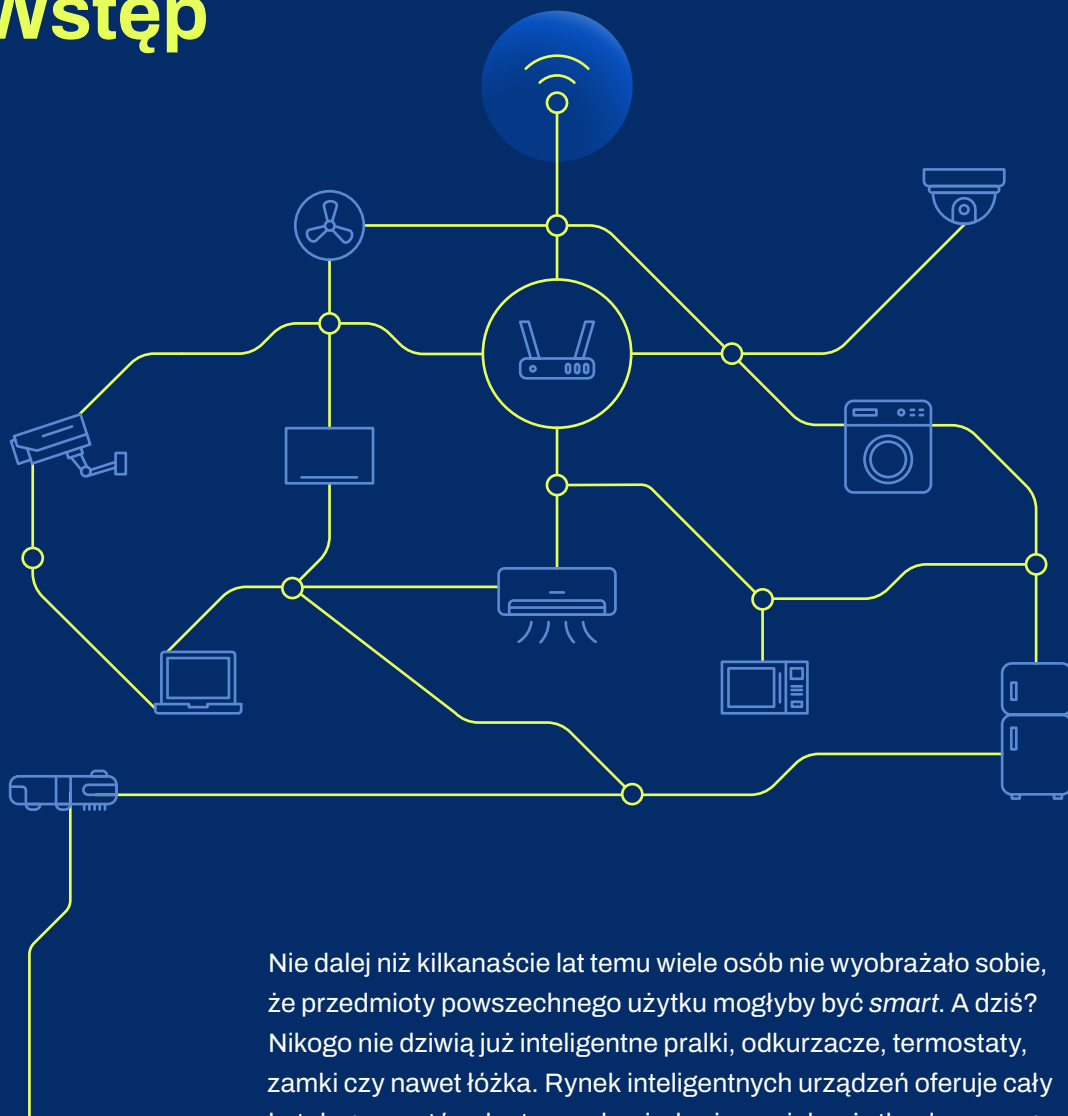
NASK



PROJEKT FINANSOWANY ZE ŚRODKÓW
MINISTERSTWA CYFRYZACJI

Publikacja wyraża jedynie poglądy autora/ów i nie może być utożsamiana z oficjalnym
stanowiskiem Ministerstwa Cyfryzacji

Wstęp



21,1 mld
urządzeń IoT
w sieci
w 2025 roku

Nie dalej niż kilkanaście lat temu wiele osób nie wyobrażało sobie, że przedmioty powszechnego użytku mogłyby być *smart*. A dziś? Nikogo nie dziwią już inteligentne pralki, odkurzacze, termostaty, zamki czy nawet łóżka. Rynek inteligentnych urządzeń oferuje cały katalog sprzętów dostępnych między innymi do użytku domowego. Według IoT Analytics liczba podłączonych do sieci urządzeń IoT (ang. *Internet of Things* – internet rzeczy) miała osiągnąć 21,1 mld na koniec 2025 roku. Prognozy tej firmy sugerują wzrost tej wartości do 39 mld w ciągu 5 lat, a za 10 lat przekroczenie 50 mld*.

* Sinha, S. (2025). State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally. *IoT Analytics*, <https://iot-analytics.com/number-connected-iot-devices/> [dostęp: 24.09.2026]



Nowinki technologiczne trafiły pod strzechy. Rozwiązania typu *smart* nie znajdują już zastosowań jedynie w firmach, coraz częściej także sprzęty domowe są wyposażone w zaawansowane rozwiązania technologiczne. Zwłaszcza pokolenie młodych dorosłych, które dorastało z technologią, podąża za trendami i chętnie sięga po kolejne udogodnienia. Jednocześnie dzięki przyjaznym użytkownikowi systemom zdalnego sterowania, w które często są wyposażone sprzęty podłączone do internetu rzeczy, osoby w każdym wieku mają szansę na czerpanie pełnymi garściami z rozwoju technologicznego.

Czy jednak, pomimo wszechobecnej dostępności inteligentnych urządzeń, jako konsumentki i konsumenci zastanawiamy się nad wyzwaniami, które niesie ze sobą ten zmieniający się świat? Problematyka bezpieczeństwa online wykroczyła poza sferę wirtualną, niepostrzeżenie wkradając się do naszych domów. Dlatego, z myślą o wszystkich użytkownikach i użytkowniczkach, którzy korzystają lub rozważają korzystanie z inteligentnych rozwiązań, powstał ten materiał. W syntetyczny sposób wyjaśnia on kluczowe pojęcia związane z urządzeniami typu *smart*, obrazuje najczęstsze zagrożenia związane z internetem rzeczy, a przede wszystkim zawiera wskazówki dotyczące tego, jak można zadbać o podstawowe kwestie związane z bezpieczeństwem online.



Kiedy możemy powiedzieć, że urządzenie jest *smart*, i czym jest internet rzeczy?



Popularność urządzeń *smart* wiąże się przede wszystkim z wygodą. Kto, wracając do domu zimową porą, nie byłby zadowolony z wejścia do mieszkania, w którym ogrzewanie włączyło się automatycznie, gdy jeszcze był w drodze, a dodatkowo odkurzenie całego domu skończyło się tuż przed otwarciem drzwi? Albo kto, jadąc na zakupy, nie chciałby uniknąć ręcznego przygotowywania listy i sprawdzania zawartości lodówki oraz dat przydatności do spożycia? Inteligentna lodówka może wykryć, jakie produkty się w niej znajdują, wskazać, które zbliżają się do końca terminu przydatności, a następnie przygotować listę brakujących artykułów.

Funkcje *smart* mogą sprawić, że niektóre codzienne czynności zostaną zautomatyzowane i możliwe do wykonania bez ingerencji właściciela czy właścicielki.

Czy jednak wszystkie elektroniczne sprzęty zasługują na przydomek *smart*? Nie każdy przedmiot, który kupujesz, nosi miano inteligentnego. Najprościej ujmując, urządzenie *smart* to takie, które zostało wyposażone w rozwiązania technologiczne umożliwiające automatyczne wykonywanie określonych działań, komunikację z innymi urządzeniami lub reagowanie na zmieniające się warunki i dane. Do realizowania tych funkcji potrzebny jest dostęp do danych, możliwość zbierania ich np. za pomocą czujników monitorujących otoczenie, a następnie analiza i przetwarzanie.

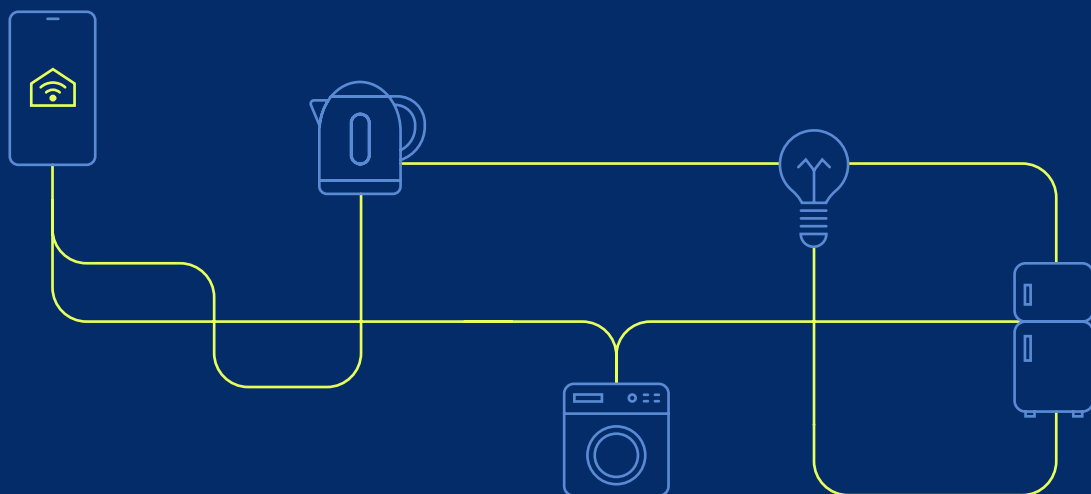


Inteligentne urządzenia

(ang. *smart devices* lub *smart objects*) to urządzenia wyposażone w zaawansowane rozwiązania technologiczne, które umożliwiają im samodzielne działanie, komunikację z innymi urządzeniami lub systemami oraz automatyzację wybranych procesów.

Urządzenia te zbierają, analizują i przetwarzają różnego rodzaju dane, aby podejmować decyzje lub wykonywać określone zadania.

Czajnik bez cyfrowych udogodnień spełnia swoją podstawową funkcję, tj. zagotowuje wodę, jednak wyposażony w funkcję *smart* i podłączony do internetu, może być włączony i wyłączony zdalnie, podgrzać wodę do wybranej temperatury czy nawet dopasować ją samemu do konkretnego napoju.



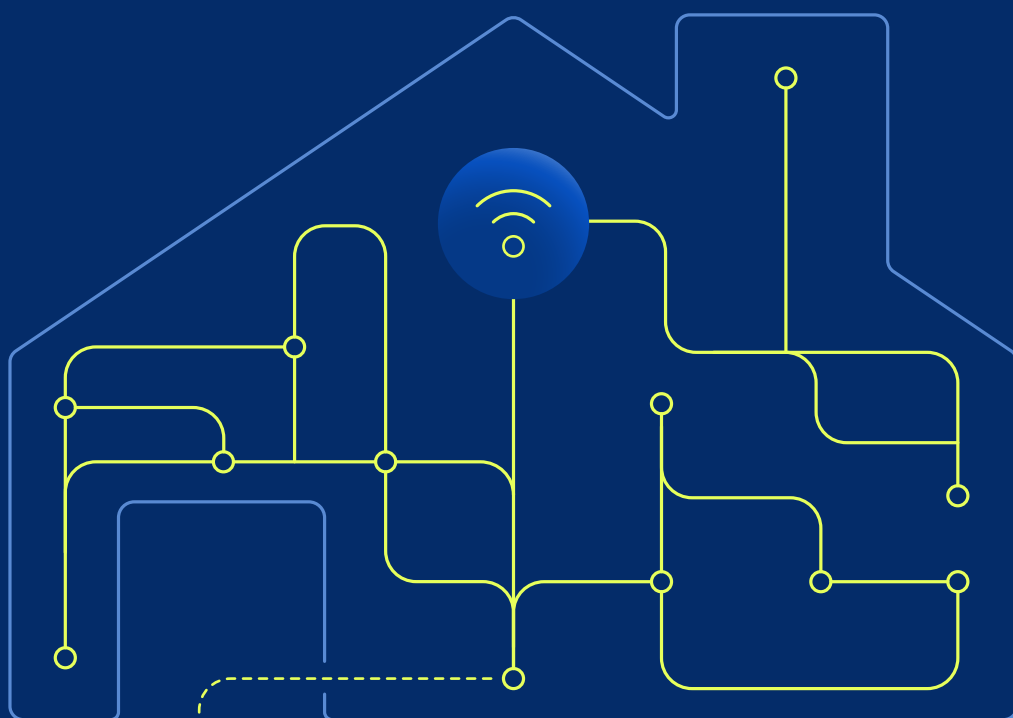
Internet Rzeczy

(ang. *Internet of Things*, IoT) to sieć połączonych ze sobą urządzeń, które mogą gromadzić dane, wymieniać się informacjami oraz współpracować ze sobą za pośrednictwem internetu lub innych sieci komunikacyjnych. Taka łączność umożliwia automatyzację wielu czynności, zdalne sterowanie oraz tworzenie inteligentnych ekosystemów urządzeń.

Dzięki internetowi rzeczy można stworzyć cały system zaprojektowany pod własne potrzeby, w którym połączone ze sobą urządzenia będą mogły być zdalnie sterowane, co pozwoli na automatyzację wielu czynności. Wyobraź sobie, że wspomniany czajnik podgrzał wodę na herbatę do zadanej temperatury i będzie ją utrzymywał do momentu, aż wrócisz do kuchni. Ty tymczasem kończysz ładować pralkę i wychodzisz z łazienki, w której światła wyłączają się same, a będąc już w kuchni, z poziomu aplikacji w telefonie wybierasz program prania. Bez pośpiechu możesz przejść do kolejnej czynności, jaką jest przygotowanie kolacji na podstawie przepisu wybranego z listy zaproponowanej przez AI – z produktów, które znajdują się w twojej lodówce.

Tak właśnie możemy pokrótce zobrazować zaledwie niewielką część możliwości, jakie dają nam inteligentne rozwiązania.

Podłączasz urządzenie do domowej sieci? Co może się stać...



Bezpieczeństwo domu można rozumieć na różne sposoby. Przed wyjściem z domu sprawdzamy np. czy wszystkie okna są zamknięte, czy drzwi balkonowe nie pozostały uchylone. A zamykając za sobą drzwi, łapiemy jeszcze odruchowo za klamkę, żeby mieć pewność, że nasz dom jest zamknięty i nie dostaną się do niego niepowołane osoby.

Kiedyś zamku broniła fosa, dzisiaj inwestujemy w technologię, która ma niejedno oblicze. Inteligentne zamki z możliwością zdalnego otwierania pomieszczeń czy dostawania się do domu za pomocą odcisku palca sprawiają, że zgubienie kluczy przestało być już problemem, kamery, które monitorują nie tylko podwórko, ale mogą być instalowane także wewnątrz mieszkania, czy różnego rodzaju czujniki, mające za zadanie informować nas o tym, że coś zostało otwarte lub został wykryty jakiś ruch... To przykłady wpływu technologii na życie codzienne i otoczenie. O czym warto pamiętać?

Zanim podłączysz urządzenie do sieci domowej, zadaj sobie pytanie:
co może się stać?

Czy zdarzyło ci się zastanawiać kiedyś nad tym, co może się stać, gdyby ktoś nieuprawniony przejął kontrolę nad twoim inteligentnym odkurzaczem lub kamerką podłączoną do sieci? Z jednej strony na myśl przychodzi utrata kontroli nad urządzeniem, a z drugiej – ktoś mógłby widzieć obraz nadawany wprost z twojego domu czy poznać cały rozkład pomieszczeń.

Urządzenia podłączone do sieci domowej nie zawsze są w pełni bezpieczne. Ich właściciele i właścicielki często przekonują się o tym dopiero po fakcie. **Coś, co z pozoru wydaje się użyteczne i bezpieczne, może w rzeczywistości stanowić zagrożenie.**



Podłączasz urządzenie do domowej sieci? Co może się stać...



Podatności

to słabości, błędy lub niezamierzone właściwości oprogramowania, firmware'u, konfiguracji, sprzętu albo usług powiązanych z urządzeniem, które mogą zostać wykorzystane przez atakujących w celu naruszenia bezpieczeństwa systemu.

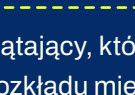
Urządzenia cyfrowe, w tym inteligentne sprzęty, nie są wolne od podatności. Innymi słowy, są jak uchylone okno, przez które przestępca może dostać się do środka, choć dom wydawał się bezpieczny, bo zamknięty na klucz.

Jeśli urządzenie jest podatne, ktoś może uzyskać do niego nieuprawniony dostęp, a dane przez nie zbierane mogą zostać przejęte lub sam sprzęt może działać nieprawidłowo.

Przykłady



Kamera bezpieczeństwa może zostać przejęta przez przestępców – oznacza to, że ktoś obcy może widzieć wszystko to, co ty do tej pory. W ten sposób potencjalni włamywacze są w stanie monitorować, kiedy ktoś jest w domu, a nawet podsłuchiwać mieszkańców lub odtwarzać dźwięki – jeśli urządzenie jest wyposażone w mikrofon albo głośnik.



Robot sprzątający, który sam odkurza lub mopuje podłogę najpierw „uczy się” rozkładu mieszkania, tj. przez wbudowane czujniki i kamery mapuje przestrzeń i zapisuje dane. W rękach przestępców jest doskonałym urządzeniem pozwalającym na poznanie dokładnego planu domu, układu pomieszczeń, a nawet rozmieszczenia mebli czy innych urządzeń. A same ustawienia czasu, w którym będzie odbywało się sprzątanie, mogą wskazywać na to, że nie ma cię wtedy w domu lub przynajmniej w konkretnym pokoju.

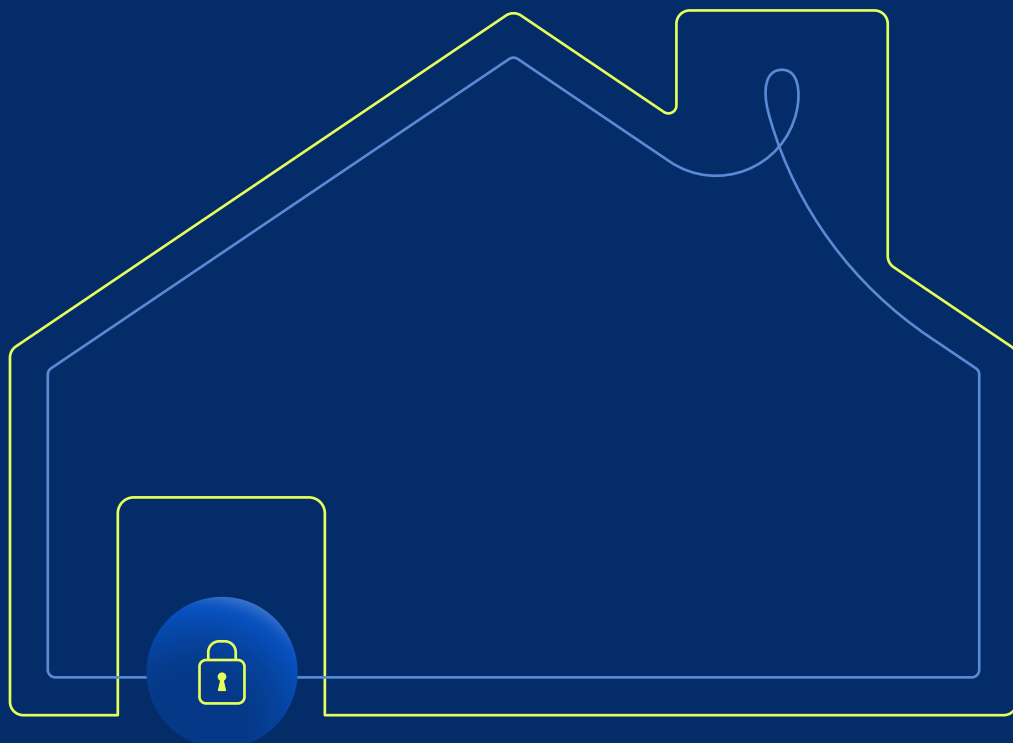


Inteligentne rozwiązania mogą otworzyć furtkę dostępu do twojego domu. Jeśli nie zadbasz o bezpieczeństwo online, to tak jakby przestępca dostał klucze do drzwi wejściowych.

Zabezpiecz się!



Zanim zdecydujesz się na inteligentne urządzenie w swoim domu



Wszystko zaczyna się od decyzji. Zanim zdecydujemy się na konkretne rozwiązanie i wybierzemy interesujący nas produkt, najczęściej oglądamy go dokładnie – możemy to zrobić na żywo, np. odwiedzając sklep stacjonarny, bądź też online, dodatkowo czytając opisy w internecie. Czasem dłuższa chwila zastanowienia może przynieść bardzo dużo korzyści – zarówno finansowych, jak i związanych z bezpieczeństwem.

To w internecie możesz zdobyć wiele kluczowych informacji na temat wymarzonego *smart* rozwiązania. Od czego zacząć i na jakie elementy zwracać uwagę?

Zacznijmy od początku

KROK 1

Przed zakupem warto zacząć od **ogólnodostępnych baz podatności**. To właśnie z nich możesz dowiedzieć się, czy urządzenie, które planujesz podłączyć do sieci domowej, miało zgłoszone luki.

CVE: Common Vulnerabilities and Exposures

Najbardziej znana, publicznie dostępna baza. Na tej stronie znajdziesz katalog dotychczas wykrytych luk bezpieczeństwa wraz z opisami. Za pomocą prostego wyszukiwania możesz sprawdzić, czy w danym urządzeniu wykryto podatności.

Pamiętaj, że brak urządzenia w bazie CVE nie jest potwierdzeniem jego bezpieczeństwa. Podatność może nie być jeszcze ujawniona, może dotyczyć komponentu użytego w urządzeniu albo występować pod inną nazwą produktu.

Warto również zweryfikować strony producentów oraz ogólnodostępne informacje publikowane w internecie dotyczące ujawnionych podatności. Pozwala to zweryfikować, czy wykryte luki zostały już potwierdzone oraz czy producent podjął działania zmierzające do ich usunięcia.

KROK 2

Kolejnym krokiem jest **zapoznanie się z opiniami innych użytkowników i użytkowników, którzy korzystali z danego urządzenia**. To właśnie z nich możesz dowiedzieć się o często występujących usterkach, jakości wsparcia technicznego czy błędach, które mogą spowodować, że urządzenie przestanie działać, i sygnalizujących je komunikatach.

KROK 3

W opiniach mogą się pojawiać także **informacje o producencie**. Czy firma reaguje na zgłaszane problemy, publikuje aktualizacje bezpieczeństwa i pomaga użytkownikom i użytkowniczkom w przypadku awarii lub wykrycia podatności?

Warto zwrócić uwagę na jakość wsparcia oferowanego przez producenta. To ważne sygnały świadczące o odpowiedzialnym podejściu do bezpieczeństwa. Zawsze dobrze zweryfikować, czy firma jest rzetelna, znana, a przede wszystkim jak długo działa na rynku.

KROK 4

Przed zakupem warto przyjrzeć się bliżej samemu urządzeniu. Najprościej jest **sięgnąć do instrukcji obsługi**, która, często niedoceniana i pomijana, w rzeczywistości może dostarczyć wielu cennych informacji. Może zapewnić wskazówki nie tylko w zakresie zasad bezpieczeństwa, ale i na temat błędów, które mogą obciążać dany sprzęt, oraz informacje o sposobach postępowania w razie pojawienia się konkretnego komunikatu. Instrukcja obsługi może okazać się niezastąpionym źródłem wiedzy.

CERT Polska

Działający w strukturach NASK/CSIRT NASK, pełni rolę koordynatora skoordynowanego ujawniania podatności. Od 2023 roku jest także partnerem programu CVE jako CNA, czyli CVE Numbering Authority – organizacja uprawniona do nadawania identyfikatorów CVE dla wybranych podatności.

Oznacza to, że każda osoba fizyczna, prawna i jednostka organizacyjna może zgłosić podatność do CSIRT NASK.

Gdzie zgłosić podatność?

Odwiedź adres:



Zgłaszanie i obsługa podatności (CVD)

Przed zakupem warto znaleźć odpowiedzi na następujące pytania:

1

Czy urządzenie zawiera podatności?

(Jakie? Czy są na bieżąco naprawiane?)

2

Czy inni użytkownicy zgłaszali problemy z urządzeniem?

(Jakiego rodzaju i czy zdarzają się często?)

3

Czy producent zapewnia aktualizacje, wsparcie i serwis

urządzenia? (Czy kontakt z obsługą klienta jest bezproblemowy?

Ile trwa obsługa zgłoszenia?)

4

Czy instrukcja obsługi jasno opisuje mogące wystąpić komunikaty

o błędach? (Czy jest ich dużo? Czy mogą rzutować na działanie

całego domu? Czy łatwo je naprawić?)

Zalecenia



Sprawdź, do kiedy producent deklaruje aktualizacje bezpieczeństwa.

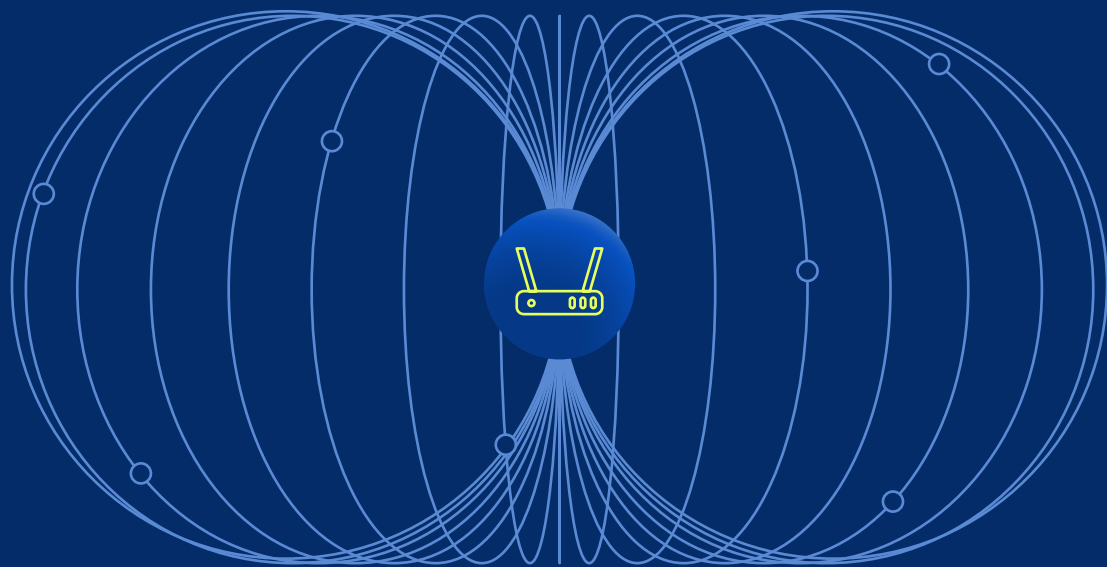


Wybieraj urządzenia z automatycznymi aktualizacjami lub jasnym mechanizmem ich instalowania.



Nie kupuj urządzeń, dla których producent nie podaje okresu wsparcia.

Zanim podłączysz urządzenie do swojej sieci



Po weryfikacji wszystkich wymienionych wcześniej elementów i znalezieniu odpowiedzi na postawione pytania dotyczące producenta i samego urządzenia oraz po dokonaniu wyboru konkretnego modelu – przychodzi moment, by podłączyć urządzenie do swojej domowej sieci i dzięki temu skorzystać ze wszystkich funkcji, które oferuje towarzysząca mu aplikacja.

To jest też moment, w którym *smart device* staje się częścią domowej codzienności i zaczyna gromadzić różnego rodzaju dane. Jeśli zostanie po prostu połączone z WI-FI, bez wcześniejszego przygotowania sieci i zabezpieczenia konta użytkownika, może okazać się, że jest jak otwarte na oścież okno, którym przestępcy dostaną się do naszego domu.

O co należy zadbać zawczasu?

Zmień domyślne hasła, np. hasło do konta administratora routera, do WI-FI i konta producenta/aplikacji, hasła domyślne samych urządzeń IoT – unikatowe, silne hasło utrudni przejęcie kontroli nad twoją siecią/urządzeniem.

Zmień domyślną nazwę swojej sieci WI-FI – utrudnisz identyfikację modelu routera przez cyberprzestępców.

Sprawdź standard zabezpieczeń swojej sieci WI-FI – jeśli jest taka możliwość, wybierz protokół WPA3, zapewniający lepszą ochronę.

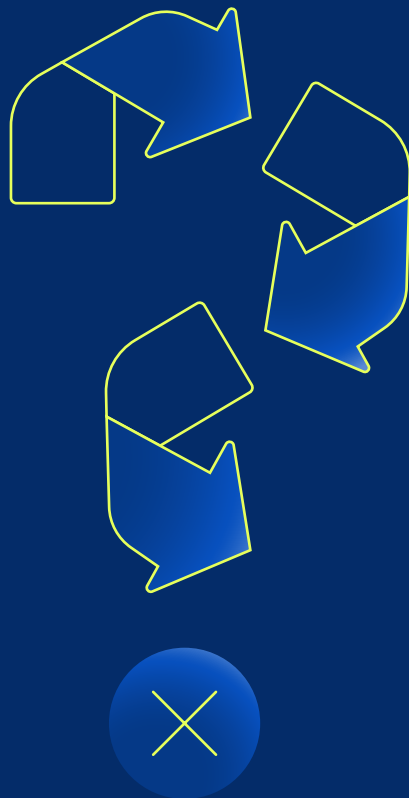
Ustaw Sieć Gości (tzw. separacja sieci) – oddzielaj urządzenia IoT od komputerów i telefonów. Rozważ konfigurację sieci VPN (ang. *Virtual Private Network*), w której znajdują się urządzenia *smart* – w ten sposób nie będą widoczne z internetu, a dostanie się do ich panelu konfiguracji będzie wymagać dodatkowego logowania.

Aktualizuj oprogramowanie routera – zadбай, żeby urządzenia, z których korzystasz, miały regularnie dostarczane aktualizacje. Pomagają one usuwać błędy, poprawiają stabilność działania urządzenia oraz zwiększają jego bezpieczeństwo poprzez eliminowanie wykrytych podatności.

Zakładając nowe konto, ustaw silne hasło i jeśli jest taka opcja, zawsze używaj uwierzytelniania dwuskładnikowego – korzystanie z urządzeń *smart* może się wiązać z koniecznością założenia konta na stronie producenta danego sprzętu. Pamiętaj, by każde z kont zabezpieczać unikalnym hasłem składającym się z co najmniej 14 znaków.

Rozważ wyłączenie funkcji zdalnego zarządzania routerem przez internet – gdy ta funkcja jest włączona, pozwala na zdalną zmianę ustawień twojej sieci. Jeśli nie korzystasz z tej opcji, warto ją wyłączyć, ponieważ może zostać wykorzystana przez cyberprzestępców do przejęcia kontroli nad routerem, a w konsekwencji także nad urządzeniami w twoim inteligentnym domu.

Urządzenia *smart* w twoim domu – co dalej?

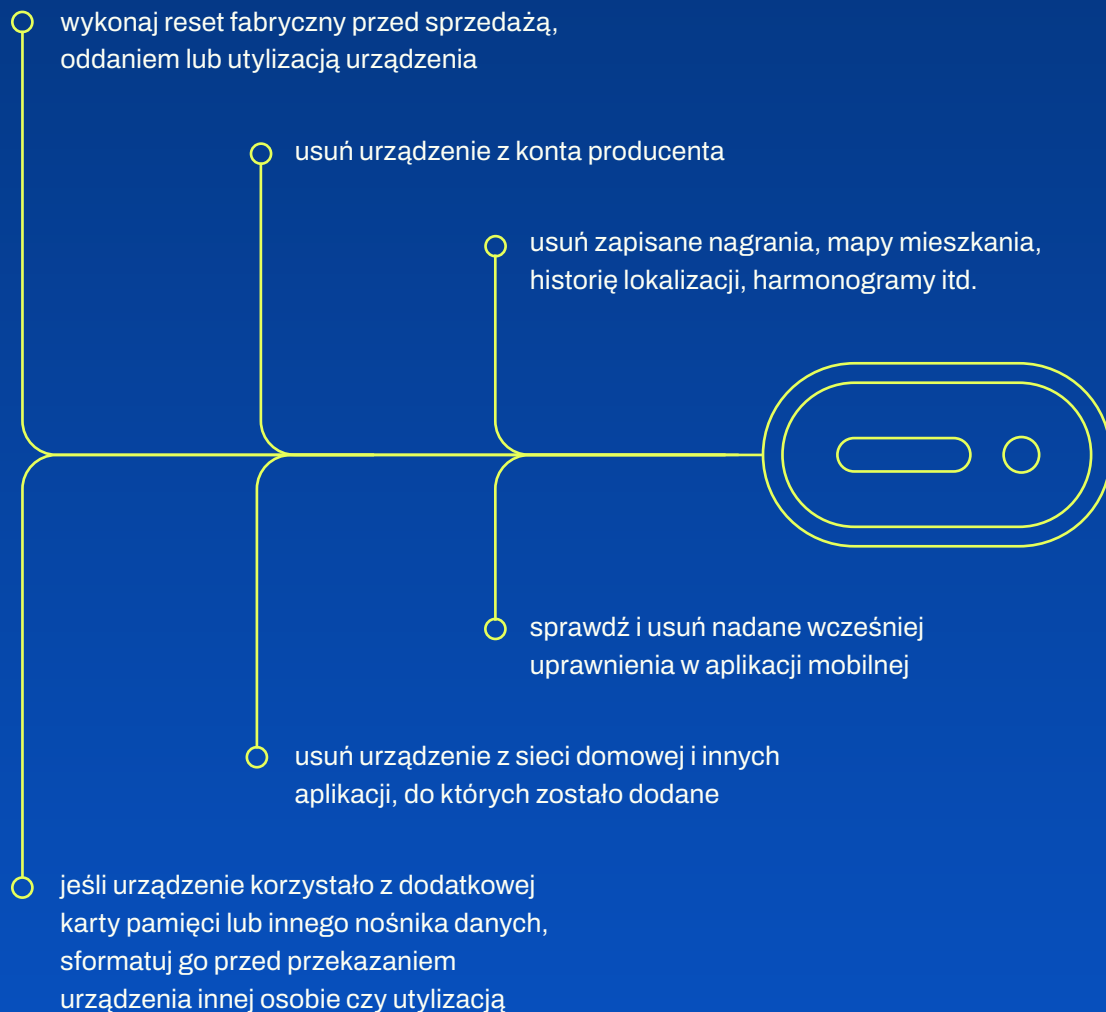


Inteligentne urządzenia na dobre zagościły w naszych domach i codziennym życiu. Korzystamy z nich przez lata, ale w końcu przychodzi moment, gdy chcemy je wymienić na nowe, przekazać komuś innemu lub oddać do recyklingu. W przypadku większości sprzętów elektronicznych zwykle tak właśnie postępujemy.

Czy w przypadku *smart devices* to dobry pomysł?

Urządzenia *smart* przechowują dane użytkownika i otoczenia, harmonogramy i zapisy aktywności czy ustawienia powiązane z naszymi kontami. Zanim oddasz albo wyrzucisz inteligentne urządzenie, pamiętaj, że do tej pory zbierało i niejednokrotnie przechowywało wiele danych o tobie. Zanim zniknie z twojego życia, zadбай przede wszystkim o cyfrowe porządk.

Pamiętaj



Fizyczne pozbycie się sprzętu powinno być poprzedzone cyfrowym resetem. Warto w trosce o własne cyberbezpieczeństwo poświęcić kilka chwil, żeby mieć pewność, że urządzenie zostało zutylizowane w sposób świadomy.

Podsumowanie

An abstract graphic consisting of numerous thin, curved blue lines that originate from the left side of the page and fan out towards the right. Interspersed among these lines are many small yellow circles and a few larger yellow rectangles, creating a sense of data flow or network connectivity.

Wiele inteligentnych urządzeń zbiera lub przetwarza dane o swoim działaniu, użytkownikach albo otoczeniu. Zakres tych danych zależy od rodzaju urządzenia, jego konfiguracji oraz wykorzystywanych usług. Dlatego tak ważny jest świadomy wybór sprzętu, weryfikacja producenta oraz dbałość o bezpieczeństwo sieci domowej i ochronę prywatności.

Internet rzeczy i inteligentne rozwiązania nie są z gruntu niebezpieczne. Wręcz przeciwnie – mogą znacząco zwiększać komfort codziennego życia. Jak w przypadku każdej *smart* technologii, kluczowe znaczenie ma jednak sposób, w jaki z niej korzystamy. Uruchomienie i korzystanie z nowego urządzenia nie powinno być otwarciem puszką Pandory. Świadomość zagrożeń, regularne aktualizacje, odpowiednia konfiguracja urządzeń i przestrzeganie podstawowych zasad cyberhigieny pozwalają ograniczyć ryzyko i sprawić, że *smart home* (inteligentny dom) będzie nie tylko wygodny i funkcjonalny, ale również bezpieczny dla wszystkich domowników.



Polecane źródła informacji



Więcej informacji o zagrożeniach i cyberhigienie
znajdziesz na naszych stronach:



bezpiecznymiesiac.pl



wiedza.cert.pl



cert.pl



nask.pl

Urządzenia IoT w domu.

Jak korzystać z nich bezpiecznie?

Zanim zdecydujesz się na inteligentne urządzenie, sprawdź czy:

- urządzenie zawiera podatności?
(Jakie? Czy są na bieżąco naprawiane?)
- inni użytkownicy zgłaszali problemy z urządzeniem?
(Jakiego rodzaju i czy zdarzają się często?)
- producent zapewnia aktualizacje, wsparcie i serwis urządzenia? (Czy kontakt z obsługą klienta jest bezproblemowy? Ile trwa obsługa zgłoszenia?)
- instrukcja obsługi jasno opisuje mogące wystąpić komunikaty o błędach? (Czy jest ich dużo? Czy mogą rzutować na działanie całego domu? Czy łatwo je naprawić?)



Zanim podłączysz urządzenie do sieci:

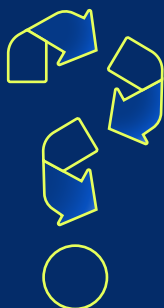
- zmień domyślne hasła – do routera, sieci WI-FI, konta producenta i samego urządzenia;
- ustaw unikalne, silne hasło do każdego konta;
- jeśli to możliwe, włącz uwierzytelnianie dwuskładnikowe;
- zmień domyślną nazwę sieci WI-FI, aby nie zdradzała modelu routera;
- korzystaj z WPA3, jeśli router i urządzenia obsługują ten standard;



- skonfiguruj osobną sieć dla urządzeń IoT, np. sieć gościnną lub VLAN;
- regularnie aktualizuj oprogramowanie routera i urządzeń;
- wyłącz zdalne zarządzanie routerem przez internet, jeśli z niego nie korzystasz;
- nie wystawiaj paneli administracyjnych urządzeń bezpośrednio do internetu.

Zanim rozstaniesz się z inteligentnym urządzeniem:

- przed sprzedażą, oddaniem lub utylizacją wykonaj reset fabryczny;
- usuń urządzenie z konta producenta;
- usuń zapisane nagrania, mapy mieszkania, historię lokalizacji, harmonogramy itd.;
- usuń urządzenie z sieci domowej i innych aplikacji, do których zostało dodane;
- sprawdź i usuń nadane wcześniej uprawnienia w aplikacji mobilnej;
- jeśli urządzenie korzystało z dodatkowej karty pamięci lub innego nośnika danych, sformatuj go przed przekazaniem urządzenia innej osobie czy utylizacją.





NASK