**Internet rzeczy – rząd Wielkiej Brytanii wydaje Kodeks Postępowania**

**Departament Cyfryzacji, Kultury, Mediów i Sportu (DCMS – Digital, Culture, Media and Sport) oraz Narodowe Centrum Bezpieczeństwa Cybernetycznego (NCSC – National Cyber Security Center) w Wielkiej Brytanii wydały niezobowiązujący Kodeks Postępowania w obszarze internetu rzeczy (IoT).**

Dokument adresowany jest do producentów urządzeń, sprzedawców detalicznych, dostawców usług IoT oraz twórców aplikacji mobilnych.

Jest to pozytywny sygnał świadczący o tym, że branża bezpieczeństwa IT nie jest jedynym podmiotem dbającym o bezpieczeństwo konsumentów. Ludzie wybierają inteligentne domy, chcąc ułatwić sobie życie, a nie po to, by tworzyć coraz bardziej stresujące środowisko narażające ich prywatność na ataki hakerów.

Rząd Wielkiej Brytanii zrozumiał zagrożenia stwarzane przez podłączone do sieci, słabo zabezpieczone urządzenia, takie jak: zabawki i elektroniczne nianie, inteligentne czujniki dymu i zamki do drzwi, inteligentne aparaty fotograficzne, telewizory i głośniki, stosowane coraz częściej w służbie zdrowia urządzenia ubieralne (ang. wearables), automatyka domowa połączona z systemami alarmowymi, urządzenia AGD (pralki, lodówki itp.) oraz elektroniczni asystenci domowi. Wytyczne dotyczą także cyfrowych usług zarządzania IoT, takich jak aplikacje mobilne, przetwarzanie i magazynowanie w chmurze oraz interfejsów API innych firm – komentuje Dawid Kraiński, Product Marketing Manager Bitdefender z firmy Marken.

W dokumencie czytamy:

*„Ponieważ coraz więcej danych osobowych powierza się urządzeniom i usługom online, cybernetyczne bezpieczeństwo tych produktów jest równie ważne, jak fizyczne bezpieczeństwo naszych domów. Celem niniejszego Kodeksu Postępowania jest udzielenie wsparcia wszystkim podmiotom zaangażowanym w rozwój, wytwarzanie i detaliczną sprzedaż produktów IoT. Publikowany zestaw wytycznych powinien z założenia gwarantować bezpieczeństwo produktów. Stosowanie się do zaleceń Kodeksu ma ułatwić ludziom zachowanie bezpieczeństwa w cyfrowym świecie”.*

Oto lista kierowanych do producentów 13 wytycznych, które mają zapewnić bezpieczeństwo urządzeń i ochronę prywatności użytkowników:

l Brak domyślnych haseł.

l Publiczne, zorganizowane wskazywanie luk w zabezpieczeniach.

l Regularne aktualizowanie oprogramowania, bezpieczny kanał przekazywania poprawek.

l Bezpiecznie przechowywane poświadczenia i inne dane krytyczne dla bezpieczeństwa.

l Bezpieczna komunikacja między maszynami (połączenia szyfrowane).

l Minimalizacja obszarów podatnych na atak.

l Integralność oprogramowania.

l Przestrzeganie przepisów dotyczących ochrony danych osobowych.

l Projektowanie urządzeń IoT odpornych na zaniki napięcia i awarie sieci.

l Monitorowanie danych telemetrycznych systemu nastawione na wykrywanie anomalii.

l Umożliwienie użytkownikom łatwego usuwania danych osobowych z usług, urządzeń i aplikacji.

l Minimalizowanie wysiłku użytkownika, związanego z instalacją, konfiguracją i korzystaniem z urządzenia.

l Kontrola poprawności danych wejściowych.

Wielka Brytania zrobiła wielki krok na drodze do ochrony prywatności i bezpieczeństwa użytkowników oraz – być może – ograniczenia dokonywanych za pośrednictwem botnetów ataków DDoS. Wśród producentów, którzy z zadowoleniem przyjęli Kodeks i zobowiązali się go wspierać, znalazły się takie firmy, jak HP Inc i Centrica Hive.

Już wcześniej w tym roku obie organizacje wydały studium *Secure by Design*, zachęcając wytwórców do uwzględnienia bezpieczeństwa już na etapie projektowania produktów.