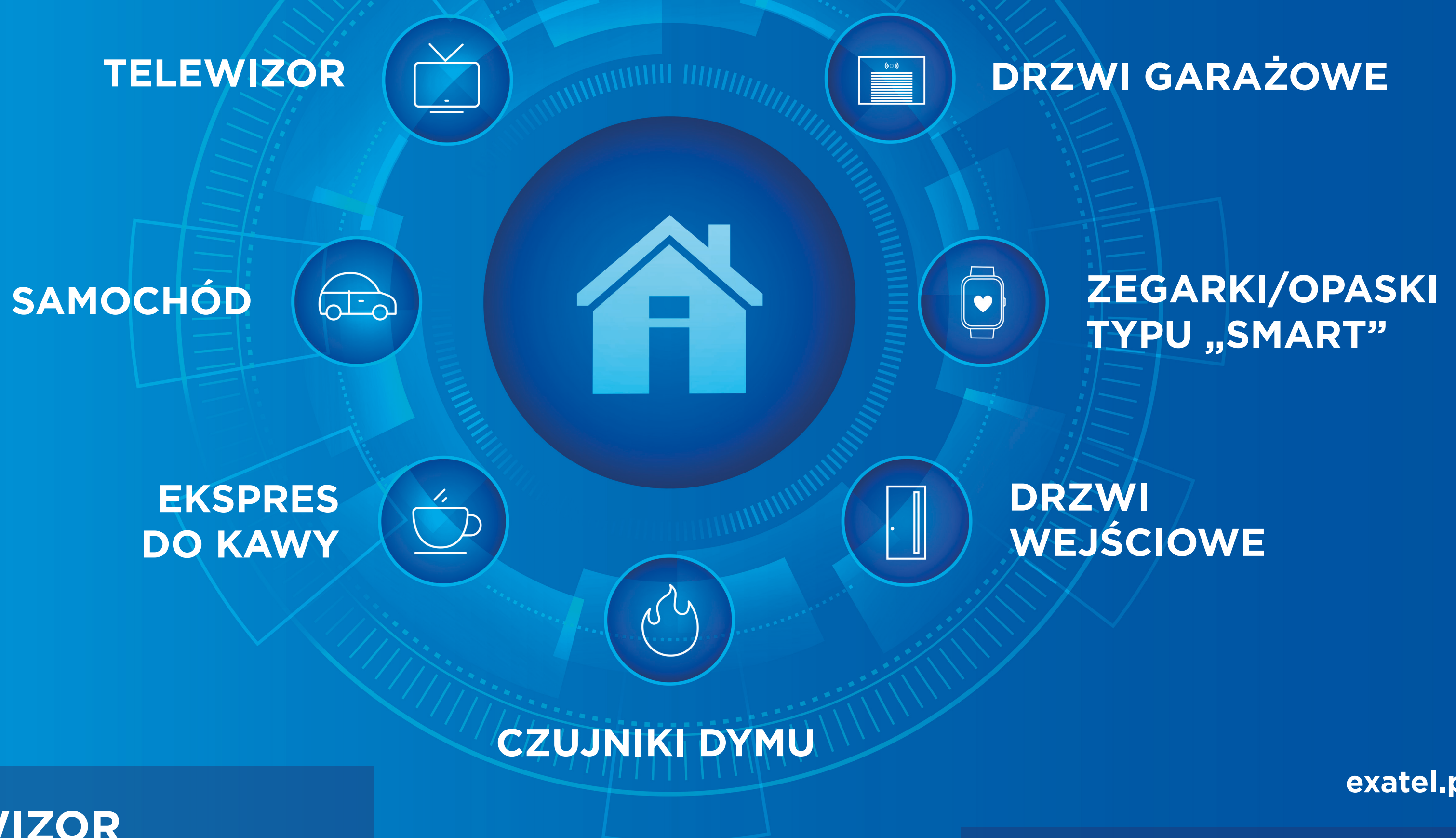


Czy wiesz, że Twoje gadżety i urządzenia domowe mogą zostać zaatakowane?

exatel.pl

TELEWIZOR

W telewizorach typu „smart” haker może zdalnie włączyć kamerę wbudowaną w TV. Podczas oglądania telewizji cyberprzestępca z każdego zakątka świata może podglądać domowników.

SAMOCHÓD

Zaatakowane systemy kontroli pojazdów mogą umożliwiać zdalne sterowanie wyświetlaczem, klimatyzacją, skrzynią biegów, a nawet hamulcami pojazdu.

EKSPRES DO KAWY

Atakujący mogą poznać dane dostępowe do domowej sieci Wi-Fi poprzez urządzenie do kawy typu „smart”.

DRZWI WEJŚCIOWE

W domach typu „smart” zdarzają się przypadki, w których hakerzy mogą zdalnie otworzyć drzwi oraz zmienić numer PIN zamków wejściowych.

DRZWI GARAŻOWE

Istnieje urządzenie znane jako HackRF, które potrafi odczytywać i odtwarzać sygnały fal radiowych. Wystarczy, że atakujący nagra sygnały z systemu otwierającego drzwi garażowe, aby je otworzyć, gdy w domu nikogo nie ma.

CZUJNIKI DYMU

Czujniki dymu dają użytkownikom możliwość ich synchronizacji z aplikacjami mobilnymi, aby powiadamiać o potencjalnych zagrożeniach. Niektóre urządzenia nie wymagają dodatkowego uwierzytelnienia, dlatego mogą być łatwym celem dla hakerów.

ZEGARKI/OPASKI TYPU „SMART”

Uprawiając sport, często udostępniamy nasze wyniki na różnych aplikacjach. Widać na nich, gdzie zaczynamy naszą trasę, co daje informację atakującym o naszym adresie zamieszkania.