BTSOFTWARE OVER DE GEVAREN VAN IOT

Wat? Komt het Chinese leger eraan?

Europa plukt nu de wrange vruchten van de van Rusland afhankelijke energiepositie waarin we ons de afgelopen jaren hebben gemanoeuvreerd. BTSoftware waarschuwt om niet in dezelfde valkuil te vallen als het gaat om China. De IoT-devices die veelal uit dat land afkomstig zijn, ogen misschien onschuldig, maar schijn bedriegt.

Met de Russische invasie in Oekraïne hebben we gezien hoe huichelachtig en leugenachtig autoritaire regimes zijn. En China is geen haar beter. Je hoeft hiervoor maar te kijken naar de opkomende sociale onrust, het falende Zero Covid-beleid, de repressie en de opkomende politieke en militaire agressie tegen Taiwan. Europa heeft zich jarenlang laten verleiden tot een energieafhankelijke positie met betrekking tot Rusland, met als desastreus gevolg dat wij nu effectief de oorlog in Oekraïne aan beide zijden financieren. En gezien de opkomende populariteit van IoT-devices is de wereld bezig om zich in eenzelfde positie ten opzichte van China te manoeuvreren. Al die schitterende micro-home-en-small-business-IT-solutions om een miniatuur SCADA-systeem op te zetten en een melding te krijgen wanneer de wasmachine klaar is met het programma, komen grotendeels uit China. Men vergeet voor het gemak vaak dat online verbinding wordt gemaakt met 'iets' in China.

> "Als Westerse maatschappij maken we ons op veel manieren kwetsbaar voor autoritaire regimes"

Misbruik

De meeste van de IoT-devices zijn betrekkelijk onschuldig en de spionagemogelijkheden maar heel beperkt. Een stap verder in de analyse laat zien, dat die onschuld ook te gebruiken is om misbruik van de maken. Unattended online updates bieden bijvoorbeeld een uitstekende mogelijkheid om achteraf aanvullende functionaliteit in te bouwen. Spionagetechnisch misschien niet zo interessant, maar wanneer bijvoorbeeld de wasmachine ineens het verwarmingselement permanent aanzet, bij voorkeur zonder dat er water in de machine zit, dan heeft dat grote gevolgen. Denk aan brand en een hoger extra verbruik. Doe dat met voldoende wasmachines en de consequenties zijn op grote schaal merkbaar. Of wat te denken van een device dat de zonnepanelen controleert? Wanneer dat er op een zonnige dag mee stopt, bestaat er eveneens een kans op oververhitting en brand. Als een groot aantal zonnepanelen, die zijn aangesloten op het elektriciteitsnetwerk, in een vast, kort ritme aan en af worden geschakeld, kan dit grote impact hebben op het publieke elektriciteitsnetwerk. En dan hebben we het nog niet gehad over de mogelijkheid dat een IoT-device als een remote hub gaat opereren, om vanuit een onverdachte locatie inbraakpogingen te ondernemen.

Vulnerable device

Na zo'n drie à vier jaar is de service van het IoT-device niet langer 'hot' en eindigt de box - nog steeds aangesloten op het publieke internet - als een vulnerable device om DDoS aanvallen mee te organiseren. Gratis en voor niets voor degene die gebruik maakt van de kwetsbaarheden in het device en de technische controle overneemt. Ook de overheden in landen als China en Rusland houden zich hiermee bezig.

Kortom, als Westerse maatschappij maken we ons op veel manieren kwetsbaar voor autoritaire regimes. Hopelijk leren we van de huidige aardgasafhankelijkheid van Rusland en vallen we niet in dezelfde valkuil als het gaat om China, dat de politieke expansie-idealen nog altijd hoog in het vaandel lijkt te hebben. ■