Veiligheid en privacy

Het grootste beveiligingsprobleem zal zijn dat als iemand een apparaat zou installeren dat is verbonden met het lokale netwerk en de gegevens van het lokale netwerk naar een extern netwerk zou sturen. Een voordeel van het bedieningssysteem is dat het een LAN-netwerk is, je kan niet het LAN-netwerk binnenkomen tenzij je een fysieke verbinding of de inloggegevens hebt van de router of raspberry pi. Dit betekent dat je fysieke toegang nodig hebt binnen de boot.



Een ander veiligheidsprobleem zou met de gebruiker hemzelf zijn, die zou de inloggegevens van de router aan de aanvaller kunnen geven doormiddel van phishing. Dit soort aanvallen heet “social engineering”. Social engineering is het extraheren van gevoelige informatie van werknemers bij een bepaald bedrijf door het gebruik van misleidende praktijken waarvan de werknemer zich niet bewust is. Deze aanvallen vereisen sterke sociale vaardigheden om succesvol te zijn en zijn vaak zeer effectief wanneer ze correct worden uitgevoerd. Uit een onderzoek van Purplesec blijkt dat 98% van cyberaanvallen afhankelijk is van social engineering als toegangspunt tot de systemen dan een bedrijf.

