



Smart Home Kühlschrank: Der Spion, der mich liebt

Eine Schwäche für französischen Käse können wir bislang vielleicht vor unserer Familie verheimlichen, vor unserem Smart Home Kühlschrank aber bald nicht mehr.

Sophos-Experte: Privathaushalte gleichen zunehmend kleinen Unternehmen.

Wiesbaden, 26. Januar 2017. Wenn es nach den Herstellern internetfähiger Kühlgeräte geht, soll der smarte Kühlschrank mit seiner intuitiven Kontrolle das neue Herzstück jeder Küche sein. Dank eines digitalen Assistenten kann man seinem Kühlgerät sagen, welche Lebensmittel es besorgen soll. Im Supermarkt selbst hilft der Blick aufs Smartphone, denn die integrierte Kühlschrankkamera verbindet sich via Wi-Fi ins heimische Netz und gibt einen Überblick über die Bestände. Smart weist der Kühlschrank nicht nur auf geringe oder leere Vorräte hin, sondern auch auf schnell zu verbrauchende Lebensmittel.

Derartige Smart-Home-Geräte waren auf der diesjährigen Consumer Electronics Show (CES), einer der weltweit größten Fachmessen für Unterhaltungselektronik, der Renner. So unterhaltsam diese Gadgets sind, sollte man sich doch im Klaren darüber sein, dass hier Nutzerdaten gesammelt werden. Auf den ersten Blick erscheint eine Einkaufshistorie harmlos. Doch die großen Datenmengen werden gespeichert, an den Hersteller gesendet, ausgewertet und können mit vielerlei anderen gespeicherten Informationen zu individuellen Profilen verknüpft werden. Ohne unser Wissen, ohne unseren Einfluss. Das ist nichts Neues. Kennen wir dieses Problem doch aus zahlreichen Diskussionen um Soziale Netzwerke wie Facebook & Co. Es gilt also Lösungen zu entwickeln, die dem Kühlschrank verbieten, Daten an den Hersteller zu senden – sofern man das möchte. Dies ist aber nur eine Seite der Misere. Weitaus kritischer ist zu sehen, dass der Kühlschrank als ein reguläres WLAN-Gerät ins häusliche Netzwerk eingebunden und damit potenziellen Angriffen durch Hacker ausgesetzt ist. Da das Kühlgerät aber selbst nicht über eine eigene Firewall oder eine andere Security-Lösung geschützt werden kann, stellt sich auch hier die Frage, wie der Anwender diese offene Tür ins Internet schließen kann.

„Smarte Geräte sind faszinierend und ich denke, dass diese sehr rasch Einzug in unser tägliches Leben halten werden“, sagt Michael Veit, Sicherheitsexperte bei Sophos in Wiesbaden. „Damit wird der Schutz von privaten Informationen für den Konsumenten immer schwieriger. Im Grunde entwickelt sich der zunehmend smarte Privathaushalt – aus IT-Security-Sicht – in Richtung einer komplexen Infrastruktur, ähnlich einem kleinen Unternehmen. Und hier helfen im Moment nur klassischer Endpoint-Schutz wie Sophos Home in Verbindung mit unserer kostenlosen Firewall-Lösung, die ursprünglich für kleine Unternehmen entwickelt wurde.“

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +172 4536839
sophos@tc-communications.de