

Ein veraltetes Smart-Home-Gerät (wie eine smarte Steckdose oder Glühbirne) ist oft das perfekte Einfallstor in ein Heimnetzwerk, da diese Geräte selten Updates erhalten und oft über schwache Sicherheitsstandards verfügen. Wenn alle Geräte im selben Netzwerk kommunizieren, sieht der Angriffsverlauf typischerweise so aus:

1. **Das Einfallstor (Initialer Kompromiss):** Ein Angreifer identifiziert eine Schwachstelle in einem veralteten Smart-Home-Gerät, beispielsweise durch eine veraltete Firmware, die über das Internet erreichbar ist, oder durch ein unsicheres Standardpasswort.
2. **Der Brückenkopf (Verankerung):** Das gehackte Gerät wird mit Schadsoftware infiziert. Der Angreifer hat nun ein aktives, unauffälliges Gerät in Ihrem lokalen Heimnetzwerk, das Sicherheitsmaßnahmen wie die Firewall des Routers von innen umgeht.
3. **Die Aufklärung (Lateral Movement):** Vom gehackten Smart-Gerät aus scannt der Angreifer das interne Netzwerk und entdeckt das NAS mit den Familienfotos sowie die Homeoffice-Laptops.
4. **Der Hauptangriff (Exfiltration & Verschlüsselung):** Der Angreifer nutzt Standardpasswörter oder ungepatchte Windows/Mac-Schwachstellen, um auf das NAS oder die Laptops zuzugreifen. Er kann nun vertrauliche Arbeitsdaten stehlen, Familienfotos kopieren oder eine Ransomware installieren, die alle Filme und Fotos auf dem NAS verschlüsselt und Lösegeld fordert.

Um diese Angriffskette zu durchbrechen, reicht ein Nachmittag. Der Fokus liegt darauf, die verletzlichsten IoT-Geräte physisch (bzw. netzwerktechnisch) von Ihren wertvollen Daten zu isolieren.

Durch das Verschieben der Smart-Home-Geräte in das Gast-WLAN (Schritt 1 & 2) dürfen diese Geräte zwar weiterhin ins Internet, um ihre Updates abzurufen oder über die App gesteuert zu werden, sie haben aber keinen Zugriff mehr auf das Hauptnetzwerk. Ein gehackter Saugroboter kann somit das NAS oder die Laptops im Hauptnetzwerk nicht einmal mehr "sehen".