OUCH! | 2018 年8月

SANS SECURITY AWARENESS

OUCH!

電腦用戶安全意識月刊

智能家居設備

什麼是智能家居設備?

傳統上, 家中只有少數設備可以連接到互聯網, 例如筆記本電腦, 智能手機或遊戲機。然而, 今天, 越來越多的設備連接到互聯網, 從燈泡和揚聲器到電視, 門鎖甚至是汽車。很快, 您家中幾乎所有設備都可以連接到互聯網。這些連接的設備通常以物聯網 (IoT) 或智能家居設備的名稱命名。雖然這些連接設備帶來了極大的便利, 但它們也帶來了獨特的危險。

有什麼問題?

連接到家庭網絡的設備越多, 出錯的可能性就越大。黑客可以對您的設備進行編程以攻擊他人, 供應商可以收集有關您活動的大量信息, 或者您的設備可能會受到感染並將您鎖在外面。製造這些設備的許多公司都沒有網絡安全經驗, 並將安全視為成本。因此, 您購買的許多設備有很少或根本沒有內置安全性。例如, 某些設備具有眾所周知的默認密碼, 或者您無法更新或設置它們。

我該如何保護自己

所以, 您可以做什麼? 我們非常希望您安全可靠地利用智能設備。這些設備可以提供讓您的生活更簡單的精彩功能。此外, 隨著技術的發展, 您可能別無選擇, 只能使用智能設備。以下是您可以採取的保護自己的關鍵步驟。

僅連接所需內容: 保護設備的最簡單方法是不將其連接到Internet。如果您不需要設備在線, 請不要將其連接到Wi-Fi網絡。您真的需要烤麵包機向您的手機發送通知嗎?

了解您已連接的設備: 您連接到家庭網絡的設備有哪些? 不確定還是不記得? 關閉無線網絡, 查看不再有效的網絡。它可能無法捕捉到所有內容, 但您會對您忘記了多少設備感到驚訝。

保持更新: 就像您的電腦和移動設備一樣, 保持您的所有設備都是最新的至關重要。如果您的設備可以選擇自動更新, 請啟用它。

密碼: 只有您知道, 才能將設備上的密碼更改為唯一且強大的密碼。您很可能只需輸入一次。記不起您所有的密碼? 別擔心, 我們也不能。考慮使用密碼管理器安全地存儲所有這些密碼。

隱私選項: 如果您的設備允許您配置隱私選項, 請限制其收集或共享的信息量。一種選擇是簡單地禁用任何信息共享功能。

供應商: 從您知道並信任的公司購買設備。尋找支持安全性的產品, 例如允許您啟用自動更新, 更改默認密碼和修改隱私設置。

始終傾聽: 如果設備可以接聽您的語音命令, 則會不斷收聽。例如, 您的Alexa和Google Home設備可以記錄敏感的會話。當您確定將設備放在家中的位置並查看隱私選項時, 請考慮這一點。

訪客網絡: 考慮將智能家居設備放在單獨的“訪客”WiFi網絡上, 而不是用於電腦和移動設備的主要WiFi網絡。這樣, 如果任何智能設備被感染, 主網絡上的電腦或移動設備仍然是安全的。

沒有理由害怕新技術, 但要了解它們帶來的風險。通過這些簡單的步驟, 您可以創建更安全的智能家居。

客座編輯

Robert M. Lee (@RobertMLee) 是SANS認證講師, 也是FOR578 - 網絡威脅情報和ICS515 - ICS主動防禦和事件響應課程的作者。Robert還是工業網絡安全公司Dragos的首席執行官和創始人。

參考資料

密碼: https://www.sans.org/u/GEB
密碼管理程式: https://www.sans.org/u/GEG
保護您的家庭網絡: https://www.sans.org/u/GEL