أمن انترنت الأشياء Security of IOT

يتزايد الاهتمام في السنوات الأخيرة بربط الأجهزة بشبكة الانترنت، والتي تعرف بإنترنت الأشياء IOT، مثل االكاميرات الأمنية، الأجهزة المنزلية الذكية، السيارات ذاتية القيادة، وأنظمة مراقبة الصحة وغيرها. ورغم أهمية هذه الأجهزة في حياتنا اليومية وفوائدها العديدة للمستخدمين، إلا إنها قد تعرضهم لمخاطر أمنية متعددة، وتجعلهم هدفاً سهلاً للمتطفلين.

فالاختراق لا يقتصر على إزعاج بسيط، بل يمتد ليشمل انتهاكات للخصوصية وسرقة للبيانات الحساسة كالمعلومات المالية والصحية. والخطر الأكثر إثارة للقلق هو تحويل أجهزتك الموثوقة إلى أدوات تجسس. يمكن للمخترقين الوصول إلى كاميرات المراقبة المنزلية، أو أجهزة مراقبة الأطفال، أو حتى المساعدات الصوتية مثل Alexa وGoogle Home. هذا يعني أنهم يستطيعون مشاهدة بث مباشر من داخل منزلك، والاستماع إلى محادثاتك الخاصة دون علمك. وقد وقعت حوادث حقيقية تمكن فيها المهاجمين من التحدث إلى أطفال عبر كاميراتهم المخترقة.

لماذا تعتبر أجهزة إنترنت الأشياء سهلة الاختراق؟

أولاً: الضعف الأمني في التصميم:
تجاهل الشركات المصنّعة لهذه الأجهزة للجوانب الأمنية أثناء التصميم، وحرصها على تلبية الطلب المتزايد على هذه الأجهزة، فهي تفتقر إلى آليات التشفير Athentication أو الجدران النارية Firewall ،مما يجعلها هدفًا سهلًا للمهاجمين .

ثانياً: البرمجيات غيرالمحدّثة:
فالثغرات في البرمجيات تظل غير معالجة لفترات طويلة، ولا تهتم الشركات المصنّعة بإصدار التحديث الذي يصلح الأخطاء والعيوب مما يشكل بوّابة للهجوم على هذه الأجهزة عبر هذه الثغرات.

ثالثاً: كلمات المرور الافتراضية:
عدم اهتمام المستخدمين بتغيير كلمة المرور الافتراضية من الشركة المصنّعة، وهي عادة ما تكون ضعيفة وسهلة التخمين، مما يسهّل على المهاجمين اقتناص هذه الفرصة واختراق الأجهزة.

رابعاً: نقص الوعي لدى المستخدمين:
وهذا السبب هو الأهم والأخطر، وذلك لكون المستخدم لا يدرك خطورة اختراق الأجهزة، وأهمية اتخاذ التدابير الأمنية التي تضمن الخصوصية والأمان.

ماهي علامات الاختراق في أجهزة انترنت الأشياء؟

مما لا شك فيه بأن خط الدفاع الأول هو الوعي ومعرفة العواقب، فهناك علامات تحذيرية قد تشير إلى اختراق أجهزتك المنزلية، مثل:

- ارتفاع حرارة الجهاز واستنزاف غير اعتيادي للبطارية
- بطء ملحوظ في الأداء أو توقف التطبيقات عن العمل بشكل متكرر
- زيادة غير اعتيادية في استهلاك بيانات الإنترنت
- تغيير في الاعدادات أو تثبيت لبرامج لم تقم بها
- أنشطة غير اعتيادية أو غير مبررة كسماع أصوات أو مشاهدة وميض

ما الذي يمكننا عمله كتدابير لضمان عدم الاختراق؟

1. الشراء من شركات مصنعة موثوقة ومهتمة بتأمين منتجاتها
2. تحديث البرمجيات بشكل دوري لإصلاح أي ثغرات
3. تغيير كلمات المرور الافتراضية
4. استخدام كلمات مرور قوية تحتوي على مزيج من الحروف الكبيرة والصغيرة والأرقام والرموز
5. تغيير كلمة المرور بشكل دوري
6. تجنب استخدام نفس كلمة المرور لأكثر من جهاز
7. استخدام تقنيات التشفير الحديثة لحماية البيانات المرسلة بين الجهاز والشبكة وضمان عدم اعتراضها
8. استخدام جدران نارية (Firewalls) لتصفية البيانات المرسلة إلى الجهاز أو منها
9. اغلاق المنافذ أو الخدمات الغير مستخدمة في حال عدم الحاجة لها
10. استخدام الشبكات الخاصة VPN لتوفير طبقة إضافية من الحماية
11. تفعيل المصادقة الثنائية عبر استخدام دليلين على هويتك
12. مراجعة أذونات التطبيقات وسياسات الخصوصية وعدم الموافقة على أي رسائل غير معروفة

من خلال ما سبق، يتضح أن الأمن والخصوصية في أجهزة انترنت الأشياء لم يعد خياراً ثانوياً، بل ضرورة أساسية في ظل الانتشار الواسع لهذه التقنيات في حياتنا اليومية وفي أماكننا الخاصة. تظل التحديات المرتبطة بحماية البيانات والأنظمة قائمة وتتطلب وعياً مستمراً وإجراءات وقائية فعالة، فتحقيق التوازن بين الاستفادة من مزايا انترنت الأشياء والحفاظ على الأمان والخصوصية يعتمد على تكاتف الجهود بين المستخدمين والشركات المصنعة، وبذلك يمكننا بناء بيئة رقمية أكثر أماناً وثقة.

م. نضال بن عيد

قسم الكمبيوتر