14 نوفمبر 2019

مجموعة السياسة الأمنية لإنترنت الأشياء ترى بأن إنترنت الأشياء ينطوي على إمكانات هائلة لتغيير العالم إلى الأفضل. فتوقعات أثر إنترنت الأشياء على الاقتصاد العالمي وعالم الإنترنت هائلة، حيث من المتوقع حدوث طفرة كبيرة في عدد أجهزة إنترنت الأشياء واستخداماتها في مجموعة واسعة من التطبيقات الجديدة المثيرة. البيان التالي موجّه إلى جميع الحكومات والمواطنين والمؤسسات ممن لديهم اهتمام في تحقيق هذه الإمكانات المتوقعة من إنترنت الأشياء.

بالنظر إلى وجود مليارات من أجهزة وتطبيقات وخدمات إنترنت الأشياء المستخدمة حاليا، إلى جانب أعداد أكبر كثيرا متوقعة مستقبلا، بات أمن إنترنت الأشياء يحتل أهمية مطلقة. فالعديد من تلك الأجهزة تفتقر إلى أبسط الخواص الأمنية، وبالتالي يمكن استغلال نقاط الضعف فيها أو الأجهزة التي تم اختراقها لتكون بمثابة معابر تُنفّذ من خلالها اعتداءات إلكترونية تلحق الضرر بالبيانات الحساسة وتهدد سلامة المستخدمين. وهذه مخاطر يلزم أن يتغلب عليها كل من يعتمد على إنترنت الأشياء، من مستخدمين وشركات.

إلا أن جهودا كبيرة جدا تُبذَل حاليا لمواجهة مخاطر إنترنت الأشياء، إلى جانب اكتشاف الفرص التي يتيحها، حيث إن تعزيز أمن إنترنت الأشياء يتيح لمستخدميه إدراك مدى فوائده. ونظرا للانتشار والأثر العالمي لشبكة الإنترنت، من المهم أن تتضافر الجهود لتحسين أمن إنترنت الأشياء.

ونرى حتى الآن أن مؤسساتنا ومنظماتنا الحكومية قد أنشأت، أو أنها في طور إنشاء، أطر أمنية قوية لإنترنت الأشياء من خلال الأبحاث المكثفة والتعاون ومنصات تضم مختلف الجهات المعنية. ويحرص أعضاء مجموعة السياسة الأمنية لإنترنت الأشياء، كل في مجال اختصاصه، على رفع معايير الممارسات الأمنية في إنترنت الأشياء. وهدفنا هو تعزيز أمن نظام إنترنت الأشياء العالمي المترابط.

رغم أن الأطر الأمنية هذه ليست متشابهة تماما، يسعى كل منها إلى تعزيز الأمن بشكل جدّي من منظور الأوضاع الإقليمية والوطنية لكل إطار. تستهدف الأطر الأمنية هذه تطبيقات مختلفة (استهلاكية، صناعية، إلخ) وأجزاء من نظام إنترنت الأشياء (الشبكات، الأجهزة، إلخ)، إلى جانب بحث مختلف السبل لتفعيل التوصيات وأفضل الممارسات. ومع ذلك، تشترك هذه الأطر الأمنية فيما بينها بمبادئ معينة موحدة:

- ضمان أخذ جوانب الأمن في عين الاعتبار في جميع مراحل التصميم والتطوير ودورة التشغيل، بما في ذلك إجراء تقييم للمخاطر، واختبار الجوانب الأمنية وإجراء تقييم لها؛
- وضمان حماية البيانات الشخصية والحيوية؛
- وتسهيل الأمر على المستخدمين لإلغاء البيانات الشخصية.

وهذه المبادئ يمكن أن تتحقق من خلال عدد من الطرق، من بينها ما يلي:

- تطبيق سياسة كشف نقاط الضعف؛
- التوضيح للمستهلكين ما هي أقل فترة زمنية يستمر خلالها الجهاز في تنزيل التحديثات الأمنية؛
- توفير آليات للتحديث الأمني للبرمجيات؛
- تعمل جهات التصنيع على بناء أجهزة تتطلب كلمات مرور أو بيانات فريدة للتحقق من هوية المستخدم؛
- حماية نقل البيانات الحساسة أمنيا [مثلا عبر وسائل مشفّرة لنقل البيانات]؛
- حفظ البيانات الحساسة أمنيا وبيانات التحقق من هوية المستخدم بشكل آمن.

لكن الأطر الأمنية هذه ما هي إلا خطوة أولى. حيث تعمل مجموعة السياسة الأمنية لإنترنت الأشياء، وكامل أعضائها، معا للتغلب على التحديات التي يواجهها الجميع عالميا، وخصوصا عدم الاتساق، في إطار توحيد الجهود الدولية المعنية بأمن إنترنت الأشياء.

وبالتطلع إلى المستقبل، سوف تواصل المجموعة بكامل أعضائها العمل معا لتنسيق وتطوير هذه الأطر الأمنية حيثما لزم الأمر، وذلك لضمان مواكبة عالم التكنولوجيا المتغير باستمرار لأجل تعزيز الثقة وزيادة التوعية بالضمانات الأمنية المرتبطة بأجهزة إنترنت الأشياء.