KHAITAN & CO ADVOCATES SINCE 1911

UPDATE

ERGO
Analysing developments impacting business

GUIDELINES FOR STRENGTHENING CYBER SECURITY - IoT DEVICES

20 March 2023

On 3 March 2023, the Department of Telecommunications (**DoT**) issued a set of advisory guidelines to machine-to-machine (**M2M**) / internet of things (**IoT**) stakeholders for securing consumer IoT (**Guidelines**). These Guidelines have been issued pursuant to a technical report released by the Telecommunication Engineering Centre titled "Code of Practice for securing Internet of Things (**IoT**)" (**CoP**). The CoP inter alia aimed at protecting the users and the networks that connect IoT devices.

Background

IoT is indisputably one of the fastest emerging technologies across the globe and has cut across various industries including healthcare, communications, energy, automobile, public safety, agriculture etc. In view of the extensive application and growing dependency of smart infrastructure, it is crucial to ensure end-to-end security of smart devices. Pertinently, the level of security required for each of such products vary across applications and associated services. In this light, the CoP was issued by TEC for securing consumer IoT products that are connected to the internet and/or home network and associated services such as inter alia connected wearable health devices, smart cameras, TVs, speakers, connected home automation and alarm systems etc.

The CoP, which postulates the concept of 'Security by Design' and implementation of the 'National Trust Centre', also sets out guidelines for securing such consumer IoT products which include setting unique passwords for IoT devices, implementing a responsible vulnerability disclosure program, securely updating software components, securely storing sensitive security parameters, ensuring protection of personal data, etc. The Guidelines issued by DoT are focused on these aspects and are issued for all stakeholders in this ecosystem, namely M2M service providers, telecom service providers, etc.

Broad guidelines for M2M / IOT stakeholders

- ***No universal default passwords:***

  Many consumer M2M / IoT devices are sold with default pre-set passwords. This has been noted as one of the major reasons for security concerns. Thus, it is advised that all consumer M2M / IoT device must have unique passwords per device. Alternatively, users may also be required to choose a password based on the prevailing best practices while obtaining such device. The passwords must not be resettable to any universal default value. As a matter of best practice, the strongest possible password must be used, as appropriate depending on the context of usage of the device. It has also been recommended that for associated web services, multi-factor authentication must be enabled, and any unnecessary user information must not be disclosed prior to authentication.

- ***Implement means to manage reports of vulnerabilities***:

  M2M / IoT stakeholders have also been advised to designate a dedicated public 'point of contact' as a part of its vulnerability disclosure policy for reporting security related concerns and issues by security researchers and others. M2M / IoT stakeholders have also been recommended to action upon disclosed vulnerabilities in a timely manner to avoid the risk of any significant harm. In order to facilitate responsible and coordinated disclosure and remediation of vulnerabilities, it has also been suggested that the cyber security community must be encouraged and rewarded for identifying and reporting vulnerabilities in the security systems of these devices.

- ***Keep the software updated***:

  The Guidelines also shed light on the importance of securely updating software in the devices and the steps to be followed in this regard. Updates should be easy to implement, made available in a timely manner, and should not adversely impact the functioning of the device. M2M IoT stakeholders must also publish an 'end-of-life' policy for end-point devices which expressly sets out the assured duration for which a device will receive software updates. For devices that cannot be physically updated, they should be isolatable and replaceable. Notably, an obligation is also placed on retailers and manufacturers to inform consumers in a timely manner whenever an update is required and to also elucidate the need for an update to such consumers.

Comment

From wrist watches that track your heart rate to factories that can be remotely controlled from a central location, IoT has penetrated numerous households and businesses today. With the remarkable features that these smart devices bring to the table, also comes the high risk of security and privacy concerns. It is now more imperative than ever to take active steps towards minimizing the threat of security attacks and system failures. In the past, the Joint Parliamentary Committee, while commenting on the previous iteration of the data protection bill, also advocated for a mechanism for formal certification process for all digital and IoT devices.

Measures such as mandatory testing and certification of telecommunication equipment (**MTCTE**) are also, inter alia, aimed at ensuring integrity and strengthening data security of such devices. While the data protection bill is round the corner, the Guidelines issued by the DoT serve as a timely and important piece of advisory to all industry stakeholders engaged in the M2M / IoT business to gear up their cyber security measures to eliminate the production of devices with weak / sub-standard security systems.

- *Harsh Walia (Partner), Shobhit Chandra (Counsel) & Sanjuktha A. Yermal (Associate)*

For any queries please contact: editors@khaitanco.com

We have updated our Privacy Policy, which provides details of how we process your personal data and apply security measures. We will continue to communicate with you based on the information available with us. You may choose to unsubscribe from our communications at any time by clicking here.