You Are The Biggest IoT Security Threat!

Security is overlooked. Kimmo Aura, Program Director, Business Finland, Connectivity from Finland's telecom acceleration program reviews IoT security today.


Kimmo Aura, Program Director, Business Finland

HELSINKI, FINLAND, August 30, 2018 /EINPresswire.com/ -- Lack of security is present in the consumer IoT market, personal and home devices and services as well as in the industrial IoT (IIoT) sector. Based on different research sources, the underlying reasons for security threats in the consumer and industrial markets are different, but the risks and damages to both can be irreparable and immeasurable in economic terms.

Consumer IoT Security

Over the next two years, the number of IoT devices entering households is predicted to climb steeply from nine devices per household currently to 500 by 2022 according to Gartner with IoT connectivity being bundled into products whether people want it or not.

According to a research funded by F-Secure, the leading cyber-security technology house, many IoT devices would go unprotected because consumers do not know how to change the manufacturers' default security settings.

> In IoT, whether consumer or industrial, humans are the biggest and hardest security problem to fix. ”
>
> *Kimmo Aura, Program Director, Business Finland*

The drive to be the first to market has meant that many manufacturers have not even considered the security implications of their devices. They have either not built appropriate security measures, use inadequate measures or, in some cases, provide no settings at all.

Of even greater concern is the potential for IoT devices to be turned into eavesdropping mechanisms that can hear and see what is going on wherever they have been deployed. Online criminals could even access and control biometric data such as fingerprints, voices and facial images stored as digital data.

Long, deliberately unwieldy and confusing terms and conditions associated with the use of devices that users are practically forced to sign up, gives manufacturers the right to collect private data and control how its device is being used. Consumers largely remain oblivious to potential implications.

Lack of awareness will also result in significant security risks to individuals since IoT devices with limited security will easily connect to home Wi-Fi networks and other radio protocols such as Bluetooth, Zigbee and Z-Wave and use those networks to link to other devices such as computers, handheld appliances and mobile phones.

Industrial IoT Security

According to the 2018 SANS Industrial IoT Security Survey Report, most organisations globally are looking at a 10 to 25 per cent growth in the number of their connected devices. This will lead to the systems that are connected to IIoT devices to double in size every three to seven years.

Consequently, enterprises see network complexity as the single biggest reason for IoT security threats. Data, firmware, embedded systems and general endpoints are identified as the most vulnerable parts of IoT systems. Systems are scattered across numerous sites hosting autonomous end-points, which make configurations difficult to manage. The SANS poll also discovered that complex systems will open a responsibility issue. IoT professionals define IIoT endpoints differently and this in turn will become the basis for confusion surrounding responsibility for IIoT security.

In IIoT, the security issue is not in the software and hardware security features. According to Tosibox, the pioneering IoT company founded to make security easy, the only way to overcome the security threats due to complexity is to minimize the amount of manual configuration work. Its solutions are unique due to highly simplified and automated network and device configuration. This minimizes manual work, and thereby reduces the likelihood of human errors.

Abstract

In IoT, whether consumer or industrial, humans are the biggest and hardest security problem to fix. End users often lack adequate tech skills, or do not care about the simplest security measures such as changing the default password. Sometimes it is product managers of device manufacturers who decide to trade security for faster time to market and higher bottom line. Sometimes it is IT managers or experts who get blown away by the gigantic complexity that this exponentially growing IoT system causes.

Ends

Mobile World Congress Americas
F-Secure and Tosibox are showcasing their IoT security solutions at the Mobile World Congress Americas in Los Angeles on September 12-14th at the Finland Pavillion (Stand 1360). Other telecom, video, cybersecurity and IoT companies showcasing at the Finland Pavilion are Bcaster, Cloudstreet, Convergentia, CreaNord, Exomi, Kaitotek and Sitowise. Finland Pavilion is organized and funded by Business Finland's Connectivity from Finland business acceleration program. Business Finland is fully-owned by the Finnish Government.

About the Author
Kimmo Aura is the Program Director at Business Finland where he heads the Connectivity from Finland program, which helps Finnish Telecom and IoT businesses accelerate international growth. Kimmo has 25 years of experience in developing international consulting businesses in Telecommunications, fiber optics, machinery, mining and management consulting. According to Kimmo, the key to success in international business growth is listening to the customers, understanding their concerns, and streamlining your own organization to fulfil the customers' needs.

About F-Secure

For three decades, F-Secure has driven innovations in cyber security, defending tens of thousands of companies and millions of people. With unsurpassed experience in endpoint protection as well as detection and response, F-Secure shields enterprises and consumers against everything from advanced cyber attacks and data breaches to widespread ransomware infections. F-Secure's sophisticated technology combines the power of machine learning with the human expertise of its world-renowned security labs for a singular approach called Live Security. F-Secure's security experts have participated in more European cyber crime scene investigations than any other company in the market, and its products are sold all over the world by over 200 broadband and mobile operators and thousands of resellers. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

About Tosibox
Tosibox was established in Oulu, Finland in 2011. Today Tosibox ecosystem solutions are used in the network infrastructure of businesses in 123 countries. The firm holds 89 global patents, has sales organisations in 29 countries and wholly-owned subsidiaries in Germany, Scandinavia and the USA.

About Business Finland
Business Finland is the Finnish innovation funding, trade, investment, and travel promotion organization, headquartered in Helsinki. Business Finland is fully owned by the Finnish Government. Business Finland employs 600 experts in 40 offices globally and in 20 regional offices around Finland. Business Finland is part of the Team Finland network.
www.businessfinland.com

Hugh Paterson
Whoosh PR
+447768175452
email us here
