Media Information

Smart Toys: Parents must know the risks and take responsibility

Stuttgart, 18.12.19. **Expert Mirko Ross explains to parents what they should absolutely pay attention to Talking dolls and app-controlled cars are all the rage. But they can do much more than inspire children. Smart toys can be used to spy on data, play advertising messages or, in the worst case, make contact with the child. Mirko Ross, an expert in cybersecurity, calls on parents to take responsibility and actively ensure the safety of interactive toys.**

Smart toys are at the top of many children's Christmas wish lists. The singing puppy and the talking teddy bear promise great fun. However, parents are often unaware that connecting toys to the Internet can pose a considerable security risk with sometimes devastating consequences. If cybercriminals succeed in taking over an IoT device, this is often a gateway to other devices and services.

"You can't be lulled by the toy look of these things," warns Mirko Ross, renowned expert and cybersecurity activist on the Internet of Things. "A talking doll is nothing more than a small computer with firmware, interfaces and the ability to process and store data. If careful attention is not paid to security when coupling it to the Internet, the doll's IT inner workings can be read or manipulated by third parties. Parents need to be aware of this and act responsibly accordingly."

The first question regarding safety arises when buying the toy. The manufacturer should meet certain security-related specifications. These include, for example, the possibility of encrypting radio connections such as Bluetooth and Wifi with a password and the regular updating of the software by upda- tes. Cheap no-name products usually do not have such security features. That's why Mirko Ross recommends spending a little more money and buying smart toys only from reputable brand-name manufacturers.

Once the toy is unpacked, the first thing parents have to do is get to grips with it. For marketing reasons, many manufacturers make commissioning the devices as easy as possible. Therefore, the toy is often already equipped with a standard password and can thus go online immediately. Attackers can obtain these passwords without any problems. It is therefore essential to invest time and patience in carefully configuring the device according to the manufacturer's specifications before using it for gaming. This also includes providing it with a secure password.

asvin GmbH
Schulze-Delitzsch-Str. 16
70565 Stuttgart
T 0711 2204093 0
F 0711 2240493 44

contact@asvin.io
www.asvin.io

@asvin_io

IBAN: DE64 6117 0024 0043 2245 00
BIC: DEUTDEDB611

Sitz Stuttgart
HRB 76700, Amtsgericht Stuttgart

A secure password must be created from a random combination of letters, numbers and special characters and must be at least 16 characters long. Under no circumstances should you use obvious and therefore insecure passwords such as "doll", "teddy bear" or the child's first name.

If the device is connected to the Internet via a router, it makes sense to select the settings so that common ports are closed, e.g. for remote maintenance access, and are thus unreachable for snooping scanners and attackers. Finally, you should clarify whether the toy is automatically supplied with updates by the manufacturer or whether you have to download updates yourself - and then do so!

Is a carefully configured smart toy really safe? Mirko Ross comments: "As long as the manufacturer is not liable for damage caused by insecure devices, the risks in the Internet of Things will not be significantly reduced. After all, as a layman, you can't assess what security-relevant vulnerabilities a piece of software has and therefore can't take appropriate measures. There are also many question marks when it comes to data protection. For example, if I download an app and, as a father, enter my personal data and that of my child, I would have serious concerns about whether the manufacturer is handling the data responsibly. In the past, the corresponding data was unfortunately very often stored and processed unencrypted in cloud servers outside Europe. If in doubt, I would rather return such a product. The only question is, how do I explain this to my child?

Mirko Ross is an iX author and founder and CEO of the start-up asvin. He is committed to security in the IoT as a member of the expert group for security in the Internet of Things of the European Network and Information Security Agency ENISA. He is also a member of the Internet Of Things Council, a global IoT think tank, and is scientifically involved with security in the Internet of Things in the EU research project IoTCrawler.

Reprint free of charge, please provide proof (print, scan, link).

Image

Contact

seidel. agentur für kommunikation
Brunnengasse 3
73650 Winterbach (Stuttgart)
T: +49 7181 / 26 29 376
E: medien@seidel-kommunikation.de