Media information Stuttgart 13.12.2019

"This is Santa Claus": Surveillance camera in children's room hacked - How can parents protect their children from attacks by hackers?

Mirko Ross, cybersecurity expert, gives the best tips in an interview

Parents around the world are shocked: As the trade magazine WIRED reported yesterday, the eight-year-old daughter of a family in Memphis, Tennessee, was harassed by a stranger via a surveillance camera from the manufacturer Ring in her child's room. The hacker announced himself with the words "I am Santa Claus" and then instructed the girl to trash her room and break the TV set.

Question: Mr. Ross, is such a hacker attack also conceivable in our children's rooms?

Mirko Ross: Unfortunately, yes, because hacker attacks on devices connected to the Internet occur everywhere in the world, and neither network operators nor legislators can really protect us against them.

Question: How is it possible for a hacker to contact a child?

Mirko Ross: Many consumers are quickly overwhelmed by the need to operate smart products securely enough to prevent access by hackers from the outside. Such access is quite easy via so-called smart toys, for example, if they are not properly secured. Smart toys are toys such as dolls or teddy bears that are equipped with microphones and sometimes cameras and are connected to the Internet via smartphone or router. The Internet connection enables them to communicate interactively with children. If such a toy or device is not protected by a secure password, it is child's play for a hacker to hack the device.
hijack. This makes it possible to spy on data, play advertising messages, film the child or, in the worst case, speak directly to him or her.

Question: What can I do as a parent to protect my child from attacks?

Mirko Ross: Parents must first be aware of the dangers. This already means when buying: Hands off cheap no-name products. It's better to buy smart toys only from reputable brand manufacturers. If I can't be sure what I'm buying, I'd personally rather do without it if in doubt.

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

Question: Is such a branded product then really safe?

Mirko Ross: I wouldn't trust that. The industry wants to make it as easy as possible to put the devices into operation. That's why the toy is often already equipped with a standard password by the manufacturer and can thus go online immediately. Attackers can obtain these passwords without any problems. For this reason, it is essential to take the time to configure the device according to the manufacturer's instructions. This also includes providing it with its own password. A secure password should be created from a random combination of letters, digits and sonder characters and should 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. In addition, someone who knows routers well should make sure that the device is not visible from the outside and thus not visible to attackers. A third important point is software updates: You should find out whether the game is automatically supplied with updates or whether you have to download the updates yourself - and then do it!

Mr. Ross, thank you for the interview!

Mirko Ross is an iX author and founder and CEO of the start-up asvin and digital worx GmbH. He is involved in IoT security 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 project coordinator in the eHealth research project MITASSIST.

Image:

Portrait Mirko Ross, CEO asvin GmbH

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

Contact:

seidel. agentur für kommunikation
Brunnengasse 3
73650 Winterbach (bei Stuttgart)
T: +40 (0)7181 / 26 29 376
E: medien@seidel-kommunikation.de