nic.br cgi.br

20 anos cert.br

Dia da Internet Segura 2018
São Paulo / SP
06 de fevereiro de 2018

Internet dos Brinquedos

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br

Internet das Coisas (IoT)

- **“Coisas” são sistemas computacionais**
  - com capacidades similares às dos dispositivos móveis, e,
  - assim como os dispositivos móveis
    - podem apresentar vulnerabilidades
    - necessitam de cuidados de segurança
- **IoT trazendo diversas novas oportunidades de negócios**
  - mas também diversos problemas de segurança
    - segurança terceirizada (“alguém se preocupará com isso”)
    - falta de autenticação
    - autenticação fraca, *backdoors* de fabricantes
    - parte de grandes ataques ocorridos nos últimos anos

Internet dos Brinquedos (IoToys)

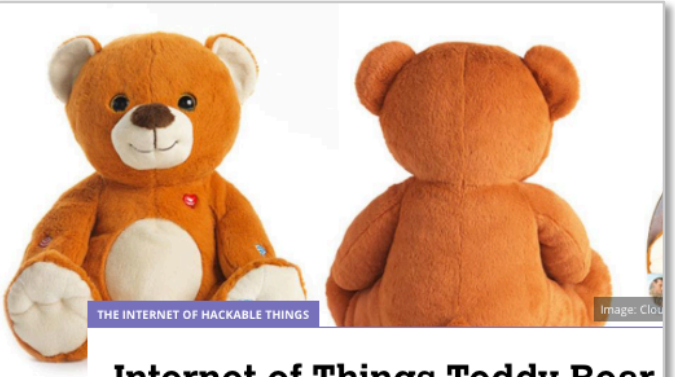
- **Brinquedos fazem parte do cenário de IoT**
- **Incorporam tecnologias que aprendem e adaptam comportamentos com base nas interações do usuário**
- **Interação:**
  - via sensores, microfones e câmeras
- **Conexão:**
  - via app, usando *bluetooth* e instalado em *tablet* ou *smartphone*
  - diretamente com a Internet
- **Dados coletados durante interação criança / brinquedo**
  - armazenados na nuvem ou em servidores da empresa
  - transmitidos a parceiros
    - por exemplo: para reconhecimento de voz

Fabricantes de brinquedos (1/2)

- **Agora também desenvolvedores de *softwares***
- **Nova área de atuação**
  - precisam adotar medidas básicas de segurança para garantir comunicações seguras e proteção das informações
  - investir na segurança do produto:
    - ter pessoal especializado
    - implementar segurança de engenharia de *software*
      - programação segura e boas práticas de desenvolvimento
    - observar os problemas já existentes e evitá-los
      - interface Bluetooth insegura, senhas fracas, falhas de autenticação, modo debug acessível, possibilidade de envio de comandos

Fabricantes de brinquedos (2/2)

- **Vulnerabilidades sempre irão existir**
  - o importante é tratá-las de forma rápida
    - quando mais rápidas as ações menores poderão ser as consequências
  - criar uma Equipe de Segurança do Produto
    - PSIRT (*Product Security Incident Response Team*)
      - para lidar com os problemas que possam acontecer
- **Problemas podem afetar seriamente a imagem da empresa**



THE INTERNET OF HACKABLE THINGS

Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings

Lorenzo Franceschi-Bicchierai
Feb 27 2017, 6:00pm

A company that sells "smart" teddy bears leaked 800,000 user account credentials—and then hackers locked it and held it for ransom.

Since Christmas day of last year and at least until the first week of January, Spiral Toys left customer data of its CloudPets brand on a database that wasn't behind a firewall or password-protected. The MongoDB was easy to find using Shodan, a search engine makes it easy to find unprotected websites and servers, according to several security researchers who found and inspected the data.

The exposed data included more than 800,000 emails and passwords, which are secured with the strong, and thus supposedly harder to crack, hashing function bcrypt. Unfortunately, however, a large number of these passwords were so weak that it's possible to crack them, according to Troy Hunt, a security researcher who maintains Have I Been Pwned and has analyzed the CloudPets data.

Spiral Toys, which appears to be based in California, could not be reached for comment. Multiple emails to different addresses were not answered, and no one from the company answered an of the phone numbers associated with them. The company appears to be in financial trouble and might be going bankrupt, given that its stock value is around zero.

https://motherboard.vice.com/en_us/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings

Call to ban sale of IoT toys with proven security flaws

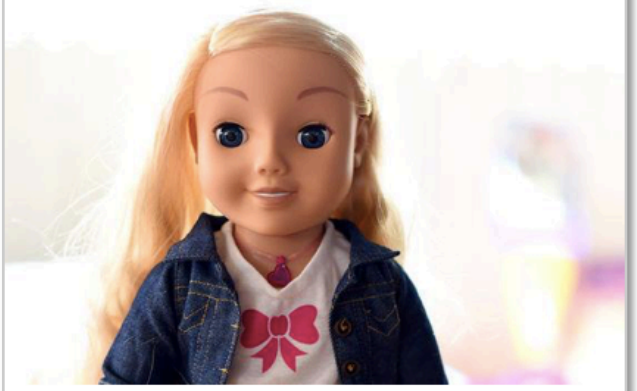
Posted Nov 15, 2017

With toys like these and other connected toys expected to be popular around Black Friday and Christmas, we're calling for smart toys to be made secure, or taken off sale entirely.

Germany bans Q&A IoT doll 'Cayla' as illegal spy device

Liam Tung (CSO Online) on 21 February, 2017 06:39

0 Comments | f 12 | in 4 |



Germany's Federal Network Agency has banned a smart doll called My Friend Cayla after deeming it a hidden surveillance device.

BRIAN BARRETT SECURITY 12.20.17 02:08 PM

DON'T GET YOUR KID AN INTERNET-CONNECTED TOY

https://www.wired.com/story/dont-gift-internet-connected-toys/
https://techcrunch.com/2017/11/15/call-to-ban-sale-of-iot-toys-with-proven-security-flaws
https://www.cso.com.au/article/614555/germany-bans-q-iot-doll-cayla-illegal-spy-device/

E como ficam os pais nesse cenário? (1/2)

- **Segurança ainda associada a riscos físicos:**
  - pontas ou extremidades cortantes
  - partes ou peças pequenas que possam se desprender com facilidade e provocar acidentes.
  - material usado na fabricação

- **Brinquedos precisam ser encarados como dispositivos móveis e necessitam de cuidados de segurança**

- **Importante conhecer os riscos para saber o que está sendo adquirido e poder avaliar se realmente vale**

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

July 17, 2017

Alert Number
I-071717(Revised)-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

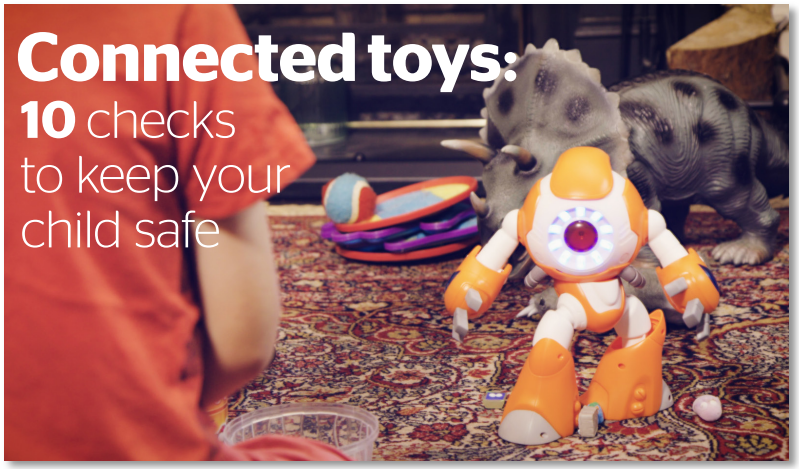
Local Field Office Locations:
www.fbi.gov/contact-us/field

CONSUMER NOTICE: INTERNET-CONNECTED TOYS COULD PRESENT PRIVACY AND CONTACT CONCERNS FOR CHILDREN

The FBI encourages consumers to consider cyber security prior to introducing smart, interactive, internet-connected toys into their homes or trusted environments. Smart toys and entertainment devices for children are increasingly incorporating technologies that learn and tailor their behaviors based on user interactions. These toys typically contain sensors, microphones, cameras, data storage components, and other multimedia capabilities – including speech recognition and GPS options. These features could put the privacy and safety of children at risk due to the large amount of personal information that may be unwittingly disclosed.

WHY DOES THIS MATTER TO MY FAMILY?

The features and functions of different toys vary widely. In some cases, toys with microphones could record and collect conversations within earshot of the device. Information such as the child's name, school, likes and dislikes, and activities may be disclosed through normal conversation with the toy or in the surrounding environment. The collection of a child's personal information combined with a toy's ability to connect to the Internet or other devices raises concerns for privacy and physical safety. Personal information (e.g., name, date of birth, pictures, address) is typically provided when creating user accounts. In addition, companies collect large amounts of additional data, such as voice messages, conversation recordings, past and real-time physical locations, Internet use history, and Internet addresses/IPs. The exposure of such information could create opportunities for child identity fraud. Additionally, the potential misuse of sensitive data such as GPS location information, visual identifiers from pictures or videos, and known interests to garner trust from a child could present exploitation risks.



Connected toys: **10** checks to keep your child safe

Any toy with Bluetooth, wi-fi connection or a mobile app that's not secured could pose a risk to your child's privacy or security. If you're shopping for a connected toy for your child, make sure you carry out these 10 vital checks:

Before buying

1. **Read the description of the connected toy carefully in the shop or online**. Find out what the toy actually does and how your child will interact with it.
2. **Check what technology it uses**. Does it require a wi-fi internet or Bluetooth connection and, more importantly, does it really need one? If you'd think twice before giving your child a internet-connected smartphone, a toy should be no different.
3. **Is there a mobile app?** If there is, what does it do and does the company talk about security features, such as usernames and passwords?
4. **Search online for the toy's name** to see if there have been any concerns raised online over its security, or how it safeguards the privacy of your child or personal data. Also, search for the manufacturer's name to see if it has had any controversies, such as a leak of customer data.
5. **Consider whether you really need a connected toy for your child**. You don't have to deny them fun, but consider whether its best to avoid having to think about internet threats until they get older.

When setting it up

1. **Submit only the minimal amount of personal data required** when setting up an account for your child. That means not too much data is exposed if things do go wrong.
2. **Read the company's T&Cs and privacy policies**, even though it's tedious. You should look for things like how your data will be stored and who has access to it. What happens if the company is hit by a cyber attack? And if a vulnerability is found with the toy, will they notify you?
3. **Download any available security updates** for the app or toy to make sure you're protected by the most recent security developments.
4. **Look for any security features available** (usually in the settings). You should be able to set passwords on any accounts, but make sure you use strong terms containing lower and upper case letters, numbers, and special characters.
5. **Keep an eye on your child when they're playing with the toy**, particularly if it can send or receive messages When they're not playing with it, make sure you turn it off.

Which? Read more at **which.co.uk/toysafety**

https://www.ic3.gov/media/2017/170717.aspx
https://www.which.co.uk/documents/pdf/connected-toy-safety-469632.pdf

E como ficam os pais nesse cenário? (2/2)

- **Antes de comprar:**
  - pesquisar pelo fabricante e pelo brinquedo
    - houve ataques recentes? se sim, como foram tratados?
    - é possível aplicar correções de segurança e atualizar o *software*?
    - são oferecidos recursos de segurança?
    - grava voz? acessa câmera? está conectado na nuvem?
  - verificar os termos de uso
    - quais informações são coletadas? como são mantidas?
  - existem meios de contatar o fabricante, em caso de problemas?
- **Durante o uso:**
  - atualizar *software* e aplicar correções de segurança
  - habilitar todas as proteções de segurança
  - restringir as informações colocados no perfil
  - supervisionar o uso
- **Desligar quando não estiver em uso**

Novas tecnologias

Novas oportunidades

Novos desafios

Até onde estamos dispostos a ir?

Obrigada

www.cert.br

miriam@cert.br

certbr

06 de fevereiro de 2018

nic.br cgi.br

www.nic.br | www.cgi.br