Mar 31, 2020, 07:15am EDT

IoT Threats And What To Do About Them

Boris Kontsevoi Forbes Councils Member
Forbes Technology Council COUNCIL POST

Boris Kontsevoi is a technology executive, President and CEO of Intetics Inc., a global software engineering and data processing company.

As the adoption of the internet of things (IoT) grows, so do legitimate security concerns about this technology. In 2018, Kaspersky honeypots identified 105 million attacks targeting smart devices.

The impact of internet-connected cars, cameras, speakers, drones, medical devices, climate control systems and similar hardware is increasing. Whether this impact will be positive or negative depends on how well we solve the IoT security problem.

This article offers a look at IoT as a double-edged sword and suggests ways we can address the challenge.

Troubling IoT Vulnerabilities That Prove The Threat Is Real

We already have a history of IoT vulnerabilities we can learn from. Here are two of the most worrying case studies:

1. Home devices eavesdropping on and manipulating people

Smart assistants like Google Home and Amazon Alexa are increasingly becoming an integral part of our lives. The technology's ability to listen and ask questions makes these devices a natural target for hackers.

The first thing that comes to mind in relation to smart speakers might be eavesdropping, but already, in 2018, researchers discovered cybersecurity problems that allowed perpetrators to phish out sensitive information, such as passwords and credit card numbers, from users.

2. Smart home hacking

Smart home systems can automate most uninspiring household tasks, freeing up your time for meaningful things. But what if someone gained control over your domestic IoT infrastructure?

This is exactly what happened to a Milwaukee couple on September 17, 2019. When they came home that day, they noticed that it was extremely hot, with a Wi-Fi-connected thermostat indicating 90 degrees Fahrenheit.

Setting the device back to room temperature did not help, as the temperature continued to rise all by itself. Soon they heard a stranger's voice and disturbing music coming from a camera in the kitchen.

The couple changed their Google Nest device network passwords, which did not fix the problem. The nightmare did not stop until their internet service provider changed their network ID.

What IoT Developers Can Do To Mitigate Risks

Developers are accountable for their products. A major breach can ruin a company's reputation and compromise the entire network, affecting thousands of users, so it is imperative for a business to take care of security.

The following are measures that you as an IoT developer might want to take:

- Start at the operating system level using the capabilities of the hardware.
- Ensure security for users every step of the way, from booting to updates.
- Stay up to date with recently discovered vulnerabilities in the underlying technology.
- Educate users. This is something Google Nest, from the example above, failed to do early. After the case went public, its spokesperson explained how to prevent such breaches — but not before it blamed consumers for "using compromised passwords (exposed through breaches on other websites)".
- Set a security check schedule, and stick to it.

What IoT Users Can Do To Protect Themselves

The consequences of an IoT breach for consumers can be irreversible and devastating.

As a user, your security is, to a great extent, in your hands. Here is what you can do about it:

- Select a product by a well-known brand. Obscure companies offer cheaper deals, but they do not care about their reputation. Although there is no 100% guarantee even with an exchange-listed brand, you can expect it to at least make an effort to protect you, along with its good name.

- Follow the security instructions from the vendor. Every IoT product has its specifics and weak points. Most of the latter are known to the software developers and manufacturers behind them. If you take the time to review the security section of the manual, you are already on the safe side.

- Know where the power button is. In most cases, you can resolve immediate issues by unplugging your device from the internet. If the problem persists, just shut it down.

- Have a separate, strong password for each of your IoT devices. Set your own password every time you purchase a new product, as default symbol combinations are commonly subject to leaks.

- Run the latest software version at all times. The invisible war between hackers and IoT vendors is in full swing. Once a vulnerability has been detected, developers will patch it and roll out a safe version. Your task here is to update as soon as possible.

- Diversify risks. Just like you separate your private life from work, keep IoT devices from these two areas independent. Then if one is compromised, the other remains untouched.

What Governments Can Do To Protect Citizens And Critical Infrastructure

Smart cities face the same threats as consumer technology, but on a much bigger scale. Even so, when people's privacy, health and lives are in danger, governments need to be concerned with their citizens' safety.

Policymakers should consider the following measures to protect citizens:

- Impose universal security standards for IoT companies.

- Set a clear certification system for IoT products to qualify as secure.

- Encourage gaining trust marks from third parties who test IoT devices.

- Ban the use of default passwords by manufacturers.
- Penalize manufacturers and developers who sell products with vulnerabilities known to date.
- Encourage manufacturers to inform users what data is collected and how it is processed.
- Support IoT vendors that educate consumers.
- Make lifetime security updates a mandatory practice for developers.

Of course, these measures come with at least one caveat: Authorities should cooperate with manufacturers and programmers in the development of new policies and regulations.

Wrap-Up

The quest for safer IoT environments involves consumers, programmers, manufacturers and governments. Various networks are increasingly interdependent, and when one of them gets hit, this also endangers the others.

Member Since 2018

Boris Kontsevoi

President & CEO

Intetics Inc.

Naples, Florida Area

Boris Kontsevoi is a founder and President of Intetics Inc., a leading global software engineering and digital transformation company. Under his leadership, a group of software engineers developed into a truly global technology company with multiple professional certifications and industry awards, including the Global Outsourcing 100, Software 500, and Global Sourcing Association best of class company.

COMPANY INFO

Intetics Inc.