January 30, 2017

Fitness trackers can be dangerous to the health of your data

As wearable devices give hackers access to personal information, consumers must demand more security

FEATURED STORY **BY RODIKA TOLLEFSON, THIRDCERTAINTY**

Wearable devices—including fitness trackers—will be the top fitness trend of 2017, driving a rapidly growing number of consumers to collect, record and analyze their health-related metrics, according to an annual trend forecast by the American College of Sports Medicine.

But cyber criminals are learning to weaponize the Internet of Things on a new, massive scale, and like most connected consumer devices, fitness trackers are not terribly secure.

Related: *As the Internet of Things expands, so do the risks*

Right now, fitness trackers are a small cog in the IoT machine. But what could happen if hundreds or thousands of employees used these easily infected devices that follow them everywhere they go, inside and outside of the network perimeter?

ABI Research estimates that more than 44 million wearable devices will be part of corporate wellness plans over the next five years.

Geoff Webb, of global software company Micro Focus, points out that the rapidly expanding space of connected devices raises concerns that are yet to be fully understood.

One is the capacity of these devices to infect one another and then form ad-hoc networks that are not connected to the internet yet allow them to talk to one another.

"Once they do that, it's really hard to see what they're up to because they're not communicating through the channels that we spent a lot of time, money and effort to secure," he says.

Another weapon in hackers' arsenal

As wearables move around, the virus could spread as easily as the flu.

"It could start an infection process that's out of control," Webb says. "If you have a population of thousands of these things, you can never catch up again, no matter how many times you send an update."

Last year, researchers at Fortinet discovered a theoretical hack in Fitbit trackers through the Bluetooth port. Although a hacker would have had to be in proximity for 10 seconds to infect the device with malware, once the device connected to a computer, it could autonomously carry out the desired action, like creating a backdoor or trojan.

Chris Clark, Synopsys principal security engineer for global solutions

With this kind of vulnerability, all it takes to introduce malware into the corporate network is one employee plugging the device into a computer USB for charging, says Chris Clark, principal security engineer for global solutions at Synopsys, which provides software testing.

"The potential for some of this smallware to infect even systems that are well-protected with anti-malware and anti-virus tools is still very high," he says.

In a highly targeted attack, a fitness tracker could be even handier: Every person's heartbeat is unique.

"The heartbeat changes over time, but a (fitness tracker) is constantly tracking it so it creates a digital signature of you," says Michael Ebert, partner and cyber practice leader at consultancy KPMG. "So you could authenticate a person walking within the perimeter just based on the tracker."

Blurring lines of medical data

Not only can they be easily hacked, but fitness trackers are not regulated in the same way as medical devices that fall under the Food and Drug Administration—which is starting to focus on the problem. Last year, the FDA issued cybersecurity guidance for manufacturers of new and existing devices.

Nor are the trackers subject to consumer protections under HIPAA, despite collecting personal health data. That means consumers don't have much control over how their data is used, and manufacturers are not required to

notify them in the event of a data breach.

"The wearables follow you around everywhere so it becomes not just a security issue, but also a privacy issue," says Craig Spiezle, executive director for the nonprofit Online Trust Alliance. Last year, OTA established the IoT Trustworthy Group, a coalition for developing security and privacy controls for connected devices.

There are many unanswered questions, Spiezle says. For example, who owns the data? What happens to the information if the individual deletes the account? What are the limitations on the data storage?

This transition to quasi-medical devices will continue, as more physicians are "prescribing" the trackers.

"Fitbit and those devices offer tremendous advantage to quality care and to continuous monitoring and measuring your performance," Ebert says.

But that means more personal data gathered about individuals by multiple entities.

"It's adding another dimension and risk footprint as they're collecting more data ... so there will (more) breaches," Spiezle says.

The OTA just released its second version of the IoT Trust Framework, which the organization hopes the IoT industry will voluntarily adopt. Among the recommended principles are full encryption, automated software and firmware patches and strong authentication.

But security features such as encryption are problematic for connected devices because additional features impact functionality, speed and battery life, as well as cost.

A trendy incentive

More compact storage, faster processing power and other improvements are making security easier to implement—and manufacturers typically respond to market pressure. What may incentivize manufacturers, ironically, is that fitness craze that employers are tapping into.

Corporate wellness programs help employers cut their health insurance costs. And according to ABI Research, early data suggests that wearable devices greatly increase participation in these programs—from 20 percent to 70 percent or more.

As manufacturers like Fitbit become more integrated into corporate infrastructure through these employee health care plans, they're under pressure to improve device security, Webb says.

"Demand from the customer base is something most organizations respond to," he says. "If you can show (employers) that you have a secure device they can bring into the organization with some degree of confidence, that would be a bigger incentive than regulation."

More stories related to IoT security:

Security of the Internet of Things takes on new urgency

Why more attacks leveraging the Internet of Things are inevitable

Healthcare data at risk: Internet of Things facilitates healthcare data breaches

Posted in Data Breach, Data Privacy, Featured Story