**Personal data breaches and securing IoT devices**

* By Damon Culbert (2019)



The Internet of Things (IoT) is taking the world by storm as interconnected devices fill workplaces and homes across the US. While the intention of these devices is always to make our lives easier, their ability to connect to the internet turns them into ticking time bombs, lying in wait until their weaknesses can be exploited by opportunistic hackers.

Personal data breaches are skyrocketing in America, increasing by 60% in the last year and by 157 percent since 2015. As our interconnectivity grows, so do the opportunities that our technology will be hacked. Since every IoT device is connected to the internet, each one is vulnerable to external access if not secured properly. In the rush to manufacture these devices and get them onto the market, security has been an afterthought which needs to be urgently addressed if the number of yearly data breaches is to be tackled.

Not only is the actual security of IoT devices under constant debate but recent news stories surrounding both the Amazon Alexa and Google Home products -- central machines to most home IoT set-ups -- show that even when used properly, the security implications of these devices can be suspect.

Though many expect IoT to revolutionize our everyday lives, the potential holes they open up in our security infrastructures could become an insurmountable problem if not dealt with soon.

**Workplace IoT**

IoT in the workplace can range from integrated systems such as air conditioning and security systems to Wi-Fi enabled coffee machines. But every point of access in a system has potential for weakness, meaning the more connected devices there are the harder it is to protect. Many believe that blockchain technology has the answer for IoT security issues due to its decentralized nature and the ability to timestamp and identify each connected device, allowing for more accurate access records and a more stable network where no central point is vulnerable.

The other key issue with workplace IoT is the necessity of regular updates to keep all devices secured. In working environments where machines are working 24/7, there is no time to take machines out of service to complete updates, meaning identified weaknesses can be left unresolved. This allows hackers multiple opportunities to exploit the insecurities in an individual device and gain access to the central network from there.

Creators of IoT devices will need to address the concerns of their consumers in order to create products which can be routinely secured and hold a high base standard of security.

**Integrated homes**

With an explosion of interconnected devices for the home comes a unique challenge that consumers are often completely oblivious to. Some IoT devices have no way to securely store the Wi-Fi password which connects them, meaning that a hacker who is able to gain access to this device can find the Wi-Fi password and exploit the entire network, risking data such as banking and personal details as well as general internet activity.

It’s unrealistic to expect consumers to use blockchain security for their washing machines and digital cameras so necessary security changes are going to have to start with the brands making the products. Ensuring that safety is properly considered before marketing any IoT device is the surest way to keep consumers’ data safe within their own network.

**Google Home and Amazon Alexa**

While not directly at the mercy of hackers, the recent revelations that recordings taken by both Amazon’s Alexa and Google Home devices have been sent to human listeners within the company raises different privacy concerns. The companies have assured that the recordings have been shared with human employees for training and research purposes but as the recent leak shows, holding personal data on recordings makes it susceptible to malicious actors online.

Amazon have taken further steps to allow users to control how Alexa stores their data and have it deleted using voice commands, making it slightly easier to protect what you say in your own home. However, many consumers buy these products without thinking of the implications of keeping a device that is always listening in their home. Companies who produce home assistant speakers need to be more transparent with how they use consumer data and take further steps to ensure no sensitive personal data is kept in recordings to help reduce the number of data breaches each year.

Trials are set to begin in the UK by Natwest bank where Google Home users will be able to check their balance with their voice. As this follows immediately on from the leaked recordings, it seems there is still little concern for the ways in which we share our personal data with the devices we use. However, online security will likely become a much bigger topic in the future as the number of internet-enabled devices rises.

The Internet of Things is proving that technology continues to advance at a rapid pace. Although consumers will need to ensure that security is a high priority in order to protect their own data and data handled by organizations, the first step must be taken by manufacturers to ensure these products are created to high security standard.

***Reference:*** [***https://betanews.com/2019/08/13/securing-iot-devices/***](https://betanews.com/2019/08/13/securing-iot-devices/)