The Internet of Things is coming with 24 Billion devices connected by 2020, but what of security, is this an opportunity or risk?

by **Marketing** on 16/02/2017

The Internet of Things (IoT) will lead to 24 billion connected devices by the year 2020 according to BI Intelligence. This growth rate signals dramatic changes for the way we live, and how brands will connect with customers and businesses manager their day to day operations.

However there is an even greater risk if security is not watertight and this is one of the primary barriers to the adoption of the Internet of Things.

Forrester predicts that more than 500,000 IoT devices will be comprised in 2017. This is a worrying statistic that highlights the fact that it I snow commonplace for attackers to access data or perform a task by impersonating a genuine user. It also stresses the importance of IoT authentication, if you're not sure which entity your communicating with then you are not able to protect your potentially sensitive data being shared. This can lead to tragic consequences such as monetary loss, confidentiality leaks, and tampering with potential health records.

An increasing number of data hacks have hit the headlines in recent years after a number of high profile breaches. The biggest data breach of all time was recently announced by Yahoo which reveals that one billion of its user accounts were hacked in 2013.

However much worse is possible, in the IoT world a breach has the potential to be life threatening. For example, a driverless car could cause a fatal accident or home medical equipment could sotp providing life sustaining aid, or over dose a patient. While in the past the main concern was typically the confidentiality of data, in the IoT it is the integrity of the data that may present a greater risk.

With IoT comes a wide range of devices, from fitness trackers and connected homes to electronic sensors gauging water levels in reservoirs, and pollution entering the rivers, each device has a digital. When these device identities are connected to user identities, the true value of the IoT is able to surface. The benefits are numerous as the high volumes of detailed data generated can also be used to gain important insights into improved efficiencies and personalised customer experiences.

With all of this data access there is a privacy conundrum. Consumers have expressed concern over who has access to the increasingly personal data that IoT devices are able to collect,

especially health-related wearables and home devices. In a recent Altimeter study, privacy concerns ranked as the top worry people have when it comes to connected devices.

Even back in the early 1990s'there were concerns over electricity meters which could monitor the power used in each house, it was seen as an 'invasion of privacy' then. Of course the supply companies knew by the extra drain on the grid when TV adverts were showing because the public got up to put their kettles on, but now things are much more personal.

Businesses must have the technology in place to manage, secure and responsibly use all of this data without violating privacy. In addition to the technical logistics involved with managing the data, organisations must ensure they're enforcing regulatory and company policies (for example ISO 27001) across all devices. They also need to consider ways to capture and enforce customer preference and consent information as data is shared with partners throughout the IoT ecosystem.

To truly address these challenges, it takes more than just adding security capabilities to existing employee identity and access management (IAM) systems. Managing identity in the IoT is fundamentally different from workforce or customer identity management. It demands an identity management (IdM) solution designed with five key security capabilities at its core. They are:

- End-to-end encryption protecting data at the network, at the device and everywhere it travels in between.
- Scalable performance and availability to handle the massive volumes of data the IoT generates.
- Privacy, preference and consent management to allow users to control their IoT experiences.
- Ability to manage relationships between devices and users over their full lifecycle.
- Adaptive authentication and policy-based data access governance for fine-grained, contextual control.

Separate from the requirement of securing devices and their data, there is an opportunity to enable new ways of authenticating users via the devices and things that will surround us. Using the smartphone for two-factor authentication is an early manifestation of this trend. The features that make the smartphone a powerful authentication factor are the same that will allow our watches, wristbands and thermostats to have an opinion on our identity (and an ability to assert that opinion).

Bak in the 1990s scientists in Russia had already worked on very personal identification processes using neural networks, for example measuring certain parameters on a person's face (Ear lobe to tip of their nose) or analysing their eye patterns. We still don't have this level of sophistication yet, but using accessories is the way we seem to be going.

The smartphone makes a powerful authentication factor because, for most users, it is always in their possession so easily accessible. But this quality of being tightly bound to a user is even more

true of the emerging class of wearables used to monitor people's fitness, sleep and other personal metrics.

When it comes to IoT, security is simply too important to be treated as an afterthought. When security features are added on as a layer to an existing identity management solution, important capabilities are sacrificed. Securing identity data for IoT environments is complex so it must be a foundational component of the IAM infrastructure.

With thanks to Hans Zandbelt Ping Identity