Computing Security
Secure systems, secure data, secure people, secure business

Be wary of wearables

Wearables are the latest big innovation for the mobile devices market. But they bring substantial security threats with them

The competition to build the greatest SmartWatch, the best SmartBand, SmartGlasses etc. puts a lot of pressure on vendors to innovate and bring unique features, treating security with low priority, warns Roman Foeckl, founder and CEO at CoSoSys and co-founder at Onyx Beacon.

"Businesses that allow their employees to bring their wearables to the workplace, or offer them to increase productivity in some cases (such as Tesco using such devices for inventory in the warehouses), are advised to treat them as any other device connected to the company network. Forecasts predict that 148 million units will be sold in 2019. They are becoming a 'must have' device for many people, as they try to motivate themselves to get more exercise done, find out more about their health etc."

IT departments are responsible for detecting connectivity between devices, to search solutions in order to secure communications and prevent attacks or other security incidents. "They should make sure that devices offered to users have remote-wipe and authentication capabilities, and that they inform users on the potential danger of their personal data being collected. Wearables could represent a perfect access point for external attackers, who can penetrate the network, exploiting the vulnerabilities of these devices."

To avoid that happening, IT departments and CSOs must take into consideration Enterprise Mobility Management (EMM) with Mobile Device Management and Mobile Application Management solutions that can control the notifications that are being sent from mobile devices to SmartWatches, for example, Foeckl advises.

"In theory, monitoring and controlling wearable tech in organisation's networks is doable and there are options on the market to secure them; besides, the experience with BYOD should be helpful, considering that WYOD is pretty similar. Once again, CSOs must be realistic and expect scepticism and even denial from employees when it comes to allow control over their personal devices."

THREAT MODELLING

While relying on firewalls alone to protect sensitive data has never worked, network controls have still been useful parts of organisations' security strategies for years, points out Amit Sethi, senior principal consultant at Cigital. "However, mobile devices and wearable devices do not exist behind corporate firewalls - at least not all the time. Employees can often be more productive, if they can access corporate data from these devices, which drives many organisations to accept or even encourage their use."

But how can organisations keep their data safe in this environment? "The first step is to perform threat modelling and architectural risk analysis on new applications, especially applications that will run on wearables that lack many of the protections and controls that we have grown accustomed to on modern platforms," says Sethi. "Of course, every wearable device is different and there is no single threat model that accurately represents a typical application running on a generic wearable device.

"Also, organisations need to focus on placing controls around sensitive data and not just around their networks... and to implement controls, such as audit trails that store details of when sensitive data is accessed, monitoring to detect anomalous behaviour and alerting to notify operators whenever suspicious data access occurs. These ideas are not new. However, organisations need to ensure that they understand the new technologies and threat landscapes in order to properly evaluate application architectures and implement the appropriate controls."

GLOBAL SUCCESS

Products such as the Apple Watch and the Fitbit have been such a global success that sales of wearable technology are expected to continue to climb throughout 2016 and beyond. A quick look at the statistics supports this, points out Mike Ellis, CEO, ForgeRock. "An NPD report found that 52% of people asked are familiar with wearable technology and, among those, a third said they would think about buying one.

"Wearable technology should be seen as a great opportunity," argues Ellis. "There are potentially negative impacts of wearable technology, such as security risks and network overload, but overall it is a great prospect. Connected device offerings will continue to grow and, with this, so will the list of commercial opportunities for UK businesses keen to invest in consumer-facing identity software."

Computing Security
Secure systems, secure data, secure people, secure business

Be wary of wearables

An increasing number of organisations today are embracing digital transformation. But with this, these organisations are in critical need of technology that securely ties together cloud, mobile and Internet of Things (IoT) offerings - including wearable devices. Identity software is becoming that critical technology, he argues. So what role does identity play?

"Identity is required to get the best out of the IoT and wearable devices. For example, if you wanted to securely share online medical data to provide better results from your health monitoring wearable, identity is imperative."

To really get the most out of wearable technology and utilise the ways in which it can empower consumers, businesses need to take a different approach to the identity services challenge. "Consumers, devices and businesses can all be connected anytime and anywhere through wearables. This means that the classic 'castle defence' approach of protecting identity data behind a firewall is rendered irrelevant. Identity systems need to handle data in real time, at Internet scale," he points out.

Not only this; they need to go further than simply switching between 'yes or no' authorisation. "Identity systems need to become business facilitators, enabling relationships between each 'thing' and its user. Identity systems must be able to understand who you are, the technology you are using and the ways you choose to interact with services," Ellis adds.

GATEWAY FOR HACKERS

"When connected to company networks, wearable devices can present potential risks: exploitable system bugs can open a gateway for hackers to pass on malware or gain access to private emails and servers," points out John Knopf, VP product management at NetMotion Wireless. "A lot of people aren't yet aware of the scale of the security risk posed by the exponential growth of connected devices, but they are vulnerable to exploitation, and often come out of the box alarmingly unprotected.

"Given that verifying the security of each individual device is time-consuming and restrictive, one important way to ensure the network is safe is to manage the traffic flow itself. By implementing per-app policies, IT can prioritise and control the flow of data to certain applications, reducing the risk of gaps in the network perimeter."

One key danger is the threat of 'evil twin' WiFi attacks, in which a hacker sets up a fake open network with an innocuous name, and then diverts information from unsuspecting users' devices when they connect, giving them access to passwords and logins. "In response to this, new 'geo-fencing' technology has been developed to help protect against such attacks - it defines access based on location, so that an employee's smartwatch, for example, could only access work emails while inside the office building, averting the danger of a remote breach."