How Location-Based IT Could Re-invent Healthcare Security

healthitsecurity.com/news/how-location-based-it-could-re-invent-healthcare-security

By Roman Foeckl of CoSoSys 8/12/2016

We have entered an age where our private data has become an all-too-easy target for malicious individuals or organizations who steal and sell this data for significant profit.

Healthcare security is especially important as a hacker made almost $1 million by selling 655,000 patient records on a dark web marketplace, including patients' full names, Social Security numbers, dates of birth, addresses and more. All of which can be used for identity theft and fraud.

RELATED ARTICLES

The numbers are staggering.

Nearly 90 percent of all healthcare organizations suffered at least one data breach in the past two years with an average cost of $2.2 million per hack, according to the Ponemon Institute.

The Institute also estimates that data breaches have cost the healthcare industry around $6.2 billion, as almost 79 percent of healthcare organizations were hit with two or more data breaches in the past two years, and 45 percent experiencing more than five breaches.

One way to address this growing issue is for organizations to implement context-aware IT policies. As the cyber-attacks become increasingly sophisticated, and insider threats increasingly present, the security tools we apply need to take into consideration an added level of security through understanding the context in which data is being used.

New technologies that utilize this contextual awareness are set to have a significant impact on securing the healthcare industry, among others. These technologies include: beacons, indoor mapping, and geofencing.

Enter the beacon

Beacons are small transmitters that constantly send a signal to any device that is listening for such a signal at a distance ranging from a few inches to a more than 70 yards. Retailers have been excited about this technology as it could mean they would be able to send a push notification about certain products on sale when the device user is in the store, or help retailers understand shopping habits in different sections of their store.

But the real benefit for healthcare institutions comes from the idea that by transmitting information in a certain range, doctors or healthcare professionals can have relevant information appear on their tablet or smartphone depending on where they are in the hospital. Conversely, the moment they are out of range of the beacon, data will automatically be removed or encrypted - ensuring data does not leave a designated area.

According to ABI Research, the total beacon shipments will surpass 400 million units by 2020. So far, retail is the dominant market beacons have entered but the number of use cases for this technology is endless.

Indoor mapping

When talking about beacon technology in IT security, it is necessary to also discuss the evolution and relevance of indoor mapping.

With augmented reality paving the way, Apple and Google have made major strides in enabling localization indoors in recent years. The technology has slowly become more ubiquitous since both companies have announced an increasing number of capabilities that let business owners map out their venues using their

iPhones. This technology has a broad range of uses, but for healthcare, it can be used in conjunction with beacon technology to secure perimeters for security applications.

Aside from the resource and improved tools that are now available to end users, the adoption of indoor mapping also comes down to how fast venue owners adapt and add the indoor maps of their venues.

Geofencing

Another way for healthcare institutions to use beacon technology is by combining it with geofencing capabilities. Geofencing is a software program feature that uses GPS or radio frequency identification (RFID) to define geographical boundaries – in other words, it acts as a virtual barrier.

As a result, by implementing geofencing, healthcare institutions keep information in by restricting access to devices or applications while inside a specified perimeter - and out - by making it impossible for devices outside the perimeter to access the network.

Brave new world for healthcare institutions

With healthcare institutions facing an increasing threat of security cyber-attacks from all sides, looking at all points of entry and exit is necessary.

Today, mobile devices are used by medical professionals with minimum control from the IT team on the data they store or share.

Certainly in many situations, Mobile Device Management (MDM) solutions are enforced but not consistently used to their full capacity.

Implementing these upcoming context-based technologies have the potential to make a substantial dent in attackers' ability to infiltrate healthcare organizations and to address the insider threats that are so risky in today's work environments.

Roman Foeckl is the CEO at CoSoSys.