BIZCOMMUNITY

Security threats of the smart city

By Perry Hutton

7 Apr 2016

Car navigation systems that can predict where and when traffic jams might occur, by siphoning data from sensors in roads and other vehicles. Cameras that can spot litter in public places and call in the cleaning crew. Self-adjusting street lamps.

These are just a few of the scenarios that could become commonplace as smart cities take hold over the next few years. Driven by rising urbanisation and fuelled by technologies such as the Internet of Things (IoT) and data analytics, smart cities are on the cusp of explosive growth. Glasgow, Barcelona, Nice, New York City, London and Singapore have already embarked on the trek. The smart city technology market could be worth $27.5 billion annually by 2023, according to Navigant Research.

Smart city initiatives are driven by public sector initiatives. However, they will have a big impact on businesses. CIOs will have to learn how to tap on the new connected city infrastructure for their business. Smart city technologies like IoT and data analytics are expected to drive innovative business ideas in the future.

But the new wave of smart city services and technologies are also expected to create new security vulnerabilities. Here are five areas CIOs should watch out for.

1. A further fragmentation of IT

The last few years saw a rapid proliferation of cloud services and mobile device adoption in the workplace. The trend has transformed business productivity, but it has also wrecked the tight-fisted control that CIOs used to be able to exert on their IT systems.

CIOs now have to grapple with the idea of employees using unsanctioned cloud services via unsecured phones to hook up to corporate servers and accessing sensitive business data. The expected explosion of IoT devices − researchers estimate that by 2020, the number of active wireless connected devices will exceed 40 billion worldwide − will result in a further fragmentation of IT in businesses.

Instead of fighting the losing battle of trying to lock down devices and services, CIOs should look at protecting the data. Look for IoT devices that offer device-to-device encryption. Consider implementing − as well as bolstering − comprehensive encryption schemes to protect data in networks, cloud services and endpoint devices.

2. Device vulnerabilities

In the past year, security researchers have exposed holes in Wi-Fi-enabled Barbie dolls, Jeep Cherokee cars, fitness trackers and other new-fangled connected devices. Fortinet's FortiGuard Labs already see IoT based attacks on the radar and happening in real time around the world. This shows the risks that are coming as toys, wearables, cars and power grids get attached to sensors that are linked to a common network and the web.

IoT will bring forth a larger surface attack. Hackers will eye IoT devices as a launching pad for ‘land-and-expand’ attacks. One scenario: hackers take advantage of vulnerabilities in connected consumer devices to get a foothold within the corporate networks and hardware to which they connect.

So how do CIOs protect against the risks of connected devices and their own IoT implementations? Short of physically separating such devices from all other network systems, they can consider deploying network-based protection schemes. Internal segmentation firewalls, or ISFWs, for instance, can mitigate the proliferation of threats inside the business network. They also need to employ an IoT network security solution which is capable of mitigating exploits against this growing and vulnerable attack surface. IoT vendors need to harden their products and develop proper product security (PSIRT) teams.

3. IoT gateways can be exploited

In a typical IoT deployment, the majority of connected devices will be always connected and always on. Unlike mobile phones and laptops, such devices are likely to go through only a one-time authentication process across multiple sessions. This will make them attractive to hackers looking to infiltrate into company networks, as it allows easy control and sniffing of traffic. Shoring up the security of the gateways that connect IoT devices is therefore a must. CIOs should map out where these gateways are and where they are linked to − they can reside internally or externally, and even be connected to IoT device manufacturers. There must also be a sound plan for updating security patches on these gateways, as well as the IoT devices.

4. Big data, more risks

If there is a constant in smart city deployments, it is that more data will be generated, processed and stored. Connected devices will generate huge data repositories. Businesses that adopt big data systems will see an even larger data deluge. Unfortunately, such data will also become attractive targets for corporate hackers.

To protect huge amounts of data with large inflows and outflows, the bandwidth capabilities of security appliances will come to the fore. And when dealing with data analytics, it often isn’t just a single data set, but multiple repositories of data that may be combined and analysed together by different groups of people. For instance, a pharmaceutical company’s research efforts may be open to employees, contractors and interns. This means individual access and auditing rights.

5. A new can of worms

New worms designed to attach to IoT devices will emerge − and they could wreak more havoc given the extended reach of the new converged networks. Conficker is an example of a worm that spread on PC's in 2008 and is still persistent and prevalent in 2016. Likewise, worms and viruses that can propagate from device to device can be expected to emerge – particularly with mobile and the Android operating system.

Embedded worms will spread by leveraging and exploiting vulnerabilities in the growing IoT and mobile attack surface. The largest botnet FortiGuard labs has witnessed is in the range of 15 million PCs. Thanks to the Internet of Things, this can easily reach in excess of 50 million if the spread of IoT worms is not properly mitigated. Patch management, and network based security inspection – particularly intrusion prevention systems or IPS – that can block IoT worms is a must.

ABOUT PERRY HUTTON

Perry Hutton, regional director of Fortinet for Africa, comes from an accounting background and has spent the last 22 years in IT, the last 10 of which have been in IT security specifically. Contact him at phutton@fortinet.com.

- Security threats of the smart city - 7 Apr 2016
- Security rules for first time cloud users - 15 Feb 2016
- 6 ½ considerations for securing the home office - 23 Jun 2015
- Health-care industry - the next cybercrime target? - 9 Mar 2015
- Securing the new era of big data - 22 Jan 2015

View my profile and articles...