BIZCOMMUNITY

Smart cities. Is it wise to get smarter?

By Simon McCullough

13 Dec 2018

We are in an era of intelligent and urgent urban innovation. Our homes are connected, our streets are thriving labyrinths of interconnectivity, and our businesses are a hive of data streaming and surveillance.

Source: pixabay.com

Communities are now emerging as sophisticated centres of technical excellence, prompting micro and macro revolutions in virtually every aspect of our lives. Across the world, digital “smartness” is either being activated, enhanced, evangelised or considered a transformative option. Is this trend a good one?

As the popularity and inevitability of smart cities expand, so too does a cybercriminal’s opportunistic attack surface. Are we now putting the public’s data and infrastructure at an unprecedented risk? Are we the authors of a 21st-century tale of two cities where one is hyperconnected and vulnerable and the other overly cautious and developmentally moribund? More importantly, what the Dickens can we do to get the balance right?

The race to evolve

Urban business-as-usual will not work. Population growth and dwindling resources are driving mass migrations to the worlds’ cities, and present infrastructures are incapable of pre-empting and adapting to the consequences – much less achieving optimal, equitable living environments in the long term.

One of the smart cities’ most compelling promises is the capacity to address traditional problems with data-driven incision, mining insights from countless sensors, interactions, and behaviours. There are numerous associated economic benefits to this technological shift. According to a recent whitepaper by ABI Research, worldwide smart city technologies could unlock more than $20 trillion in additional economic benefits in the next decade.

Using data to build a Cape Town for all

Craig Kesson 22 Nov 2018

Europe has big ambitions to take advantage. 2017 European Parliament research claims that the region already has 240 cities at over 100,000 in a population with some smart city features in place (i.e. technology to improve energy use, transport systems or other infrastructure). By the end of 2019, the Smart Cities and Communities European Innovation Partnership predicts there will be 300 smart cities in play.

A future of symbiotically connected communities, services, and processes is undeniably an admirable vision. However, with all the pressures to move at pace, there are growing concerns that cybersecurity risks are inadequately anticipated or managed.

Unfortunately, many devices, systems, and technologies powering today’s smart city dream are still being developed without appropriate security architectures or threat mitigation solutions. This short-sightedness can cause a raft of vulnerabilities leading to serious issues threatening livelihoods and, in some cases, life itself. A hacker commandeering a smart parking meter may be a nuisance but a cybercriminal infiltrating a nuclear plant could cause cataclysmic repercussions.

Lessons learned

At this year’s Black Hat conference, IBM’s X-Force Red Team examined existing municipality technologies to determine the possibility of “supervillain” style attacks.

Researches focused on four common devices and found 17 vulnerabilities, of which nine were deemed critical. One European country was using a vulnerable device to detect radiation. In the US, it was a system monitoring traffic control. The vulnerabilities in question on both occasions were not complex - the vendors simply failed to implement basic security measures.

To spook us even more, IBM’s researchers went on to simulate an attack on devices that monitor water levels in dams. In less than a minute, they were able to flood surrounding areas. The simulated hack was on a commonly used piece of smart city tech and was easy to hijack causing widespread mayhem.

Architecting the future

The UN predicts that two-thirds of the world’s population will reside in densely packed megacities by 2030. This means a mass of technology coming online fast, especially with the advent of 5G, and this could potentially fuel boundless IoT fantasies and realities.

Business leaders, tech disruptors, developers, service providers, and planners need to ramp up collaboration with industry regulators and ecosystem partners urgently to ensure appropriate rollouts of secure, seamless networks and devices. The tech industry at large should also do more to ensure the principle of ‘security-by-design’ is embraced throughout the entire infrastructure development ecosystem. Furthermore, end-to-end security has to improve, including tighter authentication of users as well as enforced policies for all communication paths. At the same time, service providers have to enhance their privacy-focused data encryption capabilities with the latest advanced software.

In summary, we need governments, city planners, and business leaders to start heeding the warnings signs of growing cyber crime and include cybersecurity experts at all stages, from design and construction to infrastructural management and beyond. We all want smarter cities, but we need to get wiser at navigating the threat landscape to stay streets ahead of cybercriminals.

ABOUT SIMON MCCULLOUGH

Major Channel Account Manager at F5 Networks

- Try to tackle cybersecurity during #RWC2019 - 20 Sep 2019
- Stay safe from cybercrime with what's left of 2019 - 30 Aug 2019
- Multi-cloud's new multiculturism - 21 Aug 2019
- A new phase of cyber warfare has begun - 7 Aug 2019
- The ABC of DevOps - 27 Jun 2019

View my profile and articles...