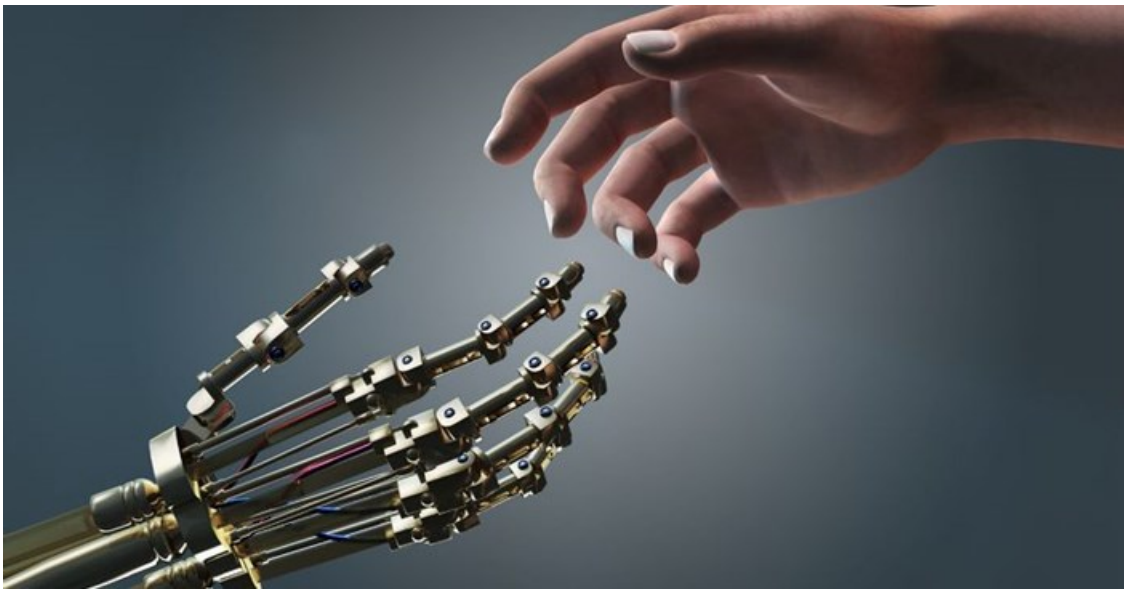
BIZCOMMUNITY

Fourth Industrial Revolution will revolutionise how we live and work

By Martin Walshaw

18 Feb 2016

You haven't been feeling well this week. You make an appointment with your doctor, who's actually a computer that assesses you and writes a prescription for flu medication. You take the prescription to your pharmacist, also a computer that quickly dispenses the drugs. The whole process takes 20 minutes and soon you're recovering in bed.



The World Economic Forum (WEF) expects the Internet of Things (IoT) to eliminate more than 50 million jobs in the next five years as technology automates more day-to-day tasks. They're calling it the Fourth Industrial Revolution, which is characterised by a fusion of technology that blurs the line between the physical and digital spheres.

While automation makes life easier in many areas - like not having to wait an hour to see your doctor - it also presents a number of risks. Privacy is becoming a luxury for consumers. We use more and more gadgets to monitor our fitness levels, automate our homes, and replace everything from cash to ID cards. More data is being collected about us than ever before. Servers in the cloud know who we are, who we communicate with and are familiar with our habits. But we don't know who is accessing this information or what they're doing with it.

Entirely new systems

When it comes to business, every industry will be affected. The IoT will give rise to entirely new systems of production, management and customer service. Competition will increase; new revenue streams will open up as others slam shut. To survive, businesses will offer more services through convenient web applications, which, if not secured properly, could provide an access point into the infrastructure for cyber criminals.

These unsecured networks and this unprotected data can be used for nefarious purposes. Take the computerised pharmacist as an example. The pharmacy recently activated an application on its website that allows patients to order their medication online.

However, the application was not properly secured, allowing a hacker to gain access to the network and compromise all prescriptions. Rather than dispensing paracetamol, the pharmacist gives you penicillin, to which you're allergic.

By automating more processes, we're placing our trust in devices and software to do the right thing. This makes security a critical element of the IoT. In a recent analysis by McKinsey, it was found that current technology could automate up to 95% of the work of doctors, nurses, paramedics, anaesthetists, aerospace engineers and hundreds of others. Imagine the catastrophic outcomes if any of these systems were to be hacked.

Security conscious

We're all responsible for security. South Africans are generally security conscious. We install burglar bars and alarm systems to protect our houses; we lock our cars after we park them. Yet, when it comes to our smartphones - arguably the most critical gadgets we own considering the amount of personal information stored on them - security is an afterthought.

We don't think twice about granting applications access to personal information, even if it doesn't make sense for them to do so - why does a photo-editing app need access to our microphone, for example. Often our devices do not have security software installed and we don't protect the devices with passwords. This is one reason why businesses should ensure that any device added to the network has security inherently built in.

As we move further into the Fourth Industrial Revolution, businesses need to protect web applications as the first point of entry into the infrastructure. To do this, they need complete visibility into the network - they need to ensure that whoever is trying to come into the network is allowed to come in, that they are who they say they are, and that they're doing what they're supposed to be doing.

Top ten vulnerabilities

Currently, many businesses don't know what normal looks like when it comes to security because they have not established security baselines. A good place to start is with the OWAST top ten web vulnerabilities. At the very least, businesses should be protecting themselves against these but this is not happening as some of these vulnerabilities have been on the list for years.

Achieving IoT security does not require network overhaul. It's likely that businesses already have infrastructure in place to support IoT security; they just need to consolidate their resources and possibly add another tool, such as SSL. An application security expert can assess your network and help you achieve a security baseline.

The Fourth Industrial Revolution will drastically change how we live and work. This change will happen suddenly and possibly without warning. Don't be caught off-guard. Start treating your devices, networks and digital identity as you would your physical security - we might not be able to tell the difference soon.

ABOUT MARTIN WALSHAW

Martin Walshaw is a senior engineer at F5 Networks and has multiple accreditation from being a CCIE to being a CISSP to being an F5 Certified Professional. His background is in security, but he has also has skills in multiple different areas including unified communications, application acceleration and optimisation.

- Visibility: your top defence against rising cyber attacks - 7 Jul 2016
- How context can provide application-centric security - 30 May 2016
- The challenges and benefits of hybrid cloud migration - 12 May 2016
- What does SSDC mean for your business? - 28 Apr 2016
- Check your blindspot on the information superhighway - 13 Apr 2016

View my profile and articles...