BIZCOMMUNITY

Securing the enterprise network with artificial intelligence

By Pieter Engelbrecht

21 Nov 2017

Artificial intelligence (AI) often throws up visions of a futuristic Earth, where self-aware robots are programmed to be ethical in their behaviour and protect human lives at all costs. It's clear that an AI future is already here, with chat bots and home assistants making the present almost as advanced as was envisaged years ago.

Image source: www.pixabay.com

But what about the role of AI in protecting the enterprise network? With the increased threat of cyber-attacks across the world, what role can AI have within data protection?

The idea of using AI in combating cyber security breaches is not a new one; however, cyber security relies on the technical ability of those implementing and designing the technology, which means experts need to work practically error-free. This undertaking is massive, and requires thousands of lines of code to be written and audited to ensure no vulnerabilities creep into the software used by businesses to protect their networks. To be in full control, businesses need to be able to learn from their existing data.

Machine learning and IoT

Machine learning, one of the key components for AI, is deployable in ways that can help companies develop technologies that can stand the malevolent AI test. This is partly thanks to the vast quantities of data residing in enterprise networks, made usable for machines to analyse and learn from. With this insight and resource, IT professionals can make a significant amount of headway in their quest for AI capable of protecting large-scale connected networks autonomously.

These networks, huge as they are now, are going to expand even further, thanks to the internet of things (IoT) becoming more prevalent in today’s society. IoT is a prodigious threat, as was shown by recent research, detailing the industries that are most affected by breaches of the technology. By 2019, up to 89% of healthcare institutions will have adopted IoT technology in one form or another, yet 89% of organisations who have already deployed the technology have suffered a breach. The research also showed that governments have suffered significant amounts of breaches – 85% in fact – but there are tactics in play and in development to help mitigate these risks.

Intent-based networking

One such strategy, intent-based networking, which is a piece of software that aids in the planning, designing, implementation and operation of networks, is already a working concept. This takes the business goals and policies as input and converts that intelligence into a network configuration, which it generates into a design and configuration.

The key for AI is to have readable and actionable data to feed off, which means networks that see a lot of data traffic can make decisions based on the behaviour of the user. A technology called user and entity behaviour analytics can do just this. Through machine learning, and the innate knowledge of knowing what to look out for, it can monitor what end-points are using the network.

Automated mitigation

On the mitigation side, with the knowledge built up through data processing and analytics, networks can be programmed to take certain actions against suspected malicious behaviour, automatically. Suspicious individuals are asked to re-authenticate and obvious dangers can be quarantined. When a breach does occur, AI can also use its knowledge to ‘score’ the risk of the threat, enabling security teams to quickly detect and respond to advanced cyber-attacks.

Artificial intelligence and machine learning can work hand-in-hand on enterprise networks, learning the various nuances of the risks associated with cyber-attacks and respond adequately. Data is key for this process but so is diligence because criminals are usually one step ahead. However, with the way the technology is progressing and the amount of data flowing through networks, there is plenty of material for AI to learn from and help keep businesses safe.

ABOUT PIETER ENGELBRECHT

Pieter Engelbrecht is the business unit manager at Aruba, a Hewlett Packard enterprise company.

- How autonomous IT and security solutions will enable proactive IT departments - 11 Apr 2019
- Creating a GDPR Compliance Framework with security tech - 26 Mar 2019
- Why are CIOs and CISOs positions becoming more challenging? - 31 Oct 2018
- Mitigate WAN complexity with SD Branch - 18 Sep 2018
- Securing the enterprise network with artificial intelligence - 21 Nov 2017

View my profile and articles...