Cybersecurity

What does it do?

Cyber security is an all-encompassing topic that over the last 10 years has become more and more prevalent in the public eye, but still retains an aspect of mystery as we transition into the age of information and technology. To give a brief overview of topic that cyber security covers, one need only make a brief list to begin to see the scope of the topic; Network security, Application Security, Identity management, database security, mobile security to name a few. However, the nature of cybersecurity is simple. To protect the integrity of networks, programs and ultimately sensitive data from damage or illegal access.

One of the most prevalent and upcoming technology for cyber security revolves around deep learning. The concept of deep learning is broader than just in regards to Cybersecurity, but essentially it’s the combination of machine learning and artificial intelligence to identify patterns through a type of deductive reasoning that uses contextual clues to indicate what is happening, this is based off and similar to the way human brains work. A current and widely used application for deep learning is image detection where each of the layers of the detects a pattern in an image that it has learned from previous images.

Two significant areas of cybersecurity that are greatly improved by deep learning is malware detection, and network intrusion. This is because systems like malware detection are currently heavily based on rule-based detection methods to deal with known threats. This leaves easily exploited holes in security due to the ability for attackers to simply tweak the malware signature to evade any current detection system. A significant benefit of this type of malware detection is that it can be applied to all types of platform including computers, smart devices and mobile phones.

By utilizing deep learning, we are able to treat malware programs like images, and apply deep learning techniques on these images to classify them as either malware or safe, this allows us to draw from commonalities in malware and to detect threats that may not fulfill all the rules of a traditional detection method.

With this being said, whilst an important aspect of cyber security is software, a lot of personal security relies on user generated passwords and protection, and it is eminently evident through repeated security breaches of peoples personal data that these methods are not adequate, as users have a tendency to use weak, easily identifiable passwords that can be breached with little to no effort for professional hacking individuals or groups. This has sparked a resurgence in hardware and multifactor authentication to add a further and less user-reliant form of protection.

Hardware authentication is both traditional, and new in many ways. It has been used by banks for a long time in the form of ATM cards, and some banks have used security tokens also, but is now more than ever accessible with the use of personal mobile devices as a secondary point of security. Companies like Google and Apple are now relying on user generated passwords, and a secondary point of verification usually in the form the user’s personal mobile device.

The impact of both of these technologies is profound on both a professional and personal level. For business’ deep learning technology is becoming near essential as we move towards a total reliance on technologically integrating business practices into the IT space. However, this progression also means significant risks, potentially crippling business’ if there are breaches to systems, which means lost revenue, and lost revenue depending on the impact can break business’ who are on the precipice.

Though the positives of deep learning cannot be stated enough, it also carries the risk of reduced jobs. As current malware and detection requires manual engineering that is consistently tweaked by software engineers. Removing the manual element allows more sophisticated and faster paced adaption to threats, but also may remove jobs that are currently essential to business’.

With regards to business’ and two factor authentication, it is common practice for major organisations to utilise key generating software and apps like authy in addition to passwords to add a secondary layer of protection for their networks. However, we may see in the near future a more biometric focused type of two factor authentication for business’ and or a wider adoption of hardware authentication in the form of keys.

On a more personal level, we may begin to see companies utilise their enormous data troves to create extremely sophisticated deep learning networks and integrate them with all future personal devices. However, in the near future, and currently we will be more impacted by the use 2 factor, and hardware authentication on more and more platforms. Companies like Mozilla and Apple are beginning to require two factor authentication for all add-on developers, and more and more companies are making 2FA a requirement, in fact google has launched an advanced protection program which utilises hardware keys that requires you to use these keys every time you want to log in to your account.

References

<https://digitalguardian.com/blog/what-cyber-security>

<https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security>

<https://www.ecpi.edu/blog/new-cybersecurity-technologies-what-is-shaking-up-the-field>

<https://www.analyticsvidhya.com/blog/2018/07/using-power-deep-learning-cyber-security/>

<https://towardsdatascience.com/malware-detection-using-deep-learning-6c95dd235432>