Cybersecurity

Introduction

Cybersecurity is the protection of all interconnected systems from threats that could breach and potentially harm hardware, software and data alike. Cybersecurity is in a constantly evolving state that challenges most organisations because of the varying degree of threats. Due to COVID-19 the need for Cybersecurity has increased as the pandemic has created more remote workforces, making them more vulnerable to cyber-attacks. The rollout of 5G has also made even more devices connected than previous times with the additional trend that most companies also have unprotected data and bad cybersecurity practices (Sobers 2021). In order to combat data breaches and cyber crime it is important to understand what Cybersecurity can do.

State of the Technology

There are many different developments in Cybersecurity but some of the more popular and rising ones today and what they can do are listed according to Writers (2021) suggestions. These are:

- Context-aware Behavioural Analytics
- Next Generation Breach Detection
- Virtual Dispersive Networking
- Smart Grid Technologies
- SAML and The Cloud
- Active Defence Measures
- Early Warning Systems

These will be stated each briefly to highlight the development and what this means for the current state of Cybersecurity which should lead into what will be developed in the future to continually combat cyber warfare.

Context-aware Behavioural Analytics

Context-aware security is defined according to Avivah Litan of Gartner, as a system of fail-safes deployed to differentiate normal and abnormal anamolies (Donohue 2014). Basically, the security relies on the use of situational information such as identity, geolocation, time of day or type, to track whether a breach has occurred through the unusual behaviours of a user (Botelho 2021). Technologies that are in development according to Donohue (2014) for it are:

- Bioprinting – being able to track such things as how hard and fast the typing of employees are.
- Mobile location tracking – being able to track whether mobile devices are logging into several accounts.
- Behavioural profiles – being able to track behaviour changes in the use of equipment.

- Third-party big data – alerted to false procedures through revealing data and where it is located.
- External threat intelligence – being able to gather intelligence through other threats.

Next Generation Breach Detection

Breach detection according to Eshel et al.,(2014) has changed from being focused as a first line of defense and actually focuses on defending the system once the hacker is inside. It takes the approach of combining behavioural analytics, machine learning and other tools to identify the traces that the hacker has left behind. Effectively being able to pick out strange movements and changes that will occur in the data and notifying the users (Writers 2021).

Virtual Dispersive Networking

VDN takes Man-in-the-Middle (MiM) attacks and makes them harder to decrypt (Writers 2021). These cyber-attacks are basically moments of when a hacker can monitor, alter or intersect within a communication between sender and receiver. According to Forbes (2014) Dispersive Technologies developed VDN to split the communication into multiple parts, encrypts those individually and routes them across multiple network platforms like how military radio is distributed.

Smart Grid Technologies

Smart Grid systems emerged in electrical infrastructure to improve operations and improve the transmission, and distribution of resources (Westlund 2007). Smart Grids are continually expanding into more than just energy and so has opened problems in cybersecurity for these industries. In response, the Department of Energy (2014) are few of the many who are developing means to combat breaches, in example:

- Padlock – gateway which establishes encrypted communications between stations and field devices.
- Watchdog – switch that manages pack inspection for the control system LAN.
- SIEGate – Secure Information Exchange Gateway is an information protocol that provides security on transmission systems.
- NetAPT – software that enables utilities to map out their control system.

SAML and The Cloud

Security Assertion Markup Language (SAML) is an XML-based open data format used to allow authentication and authorization of credentials to service providers (Petters 2020). On its own it is not sufficient however it is being combined with SSO, encryption and intrusion detection to protect data existing in the cloud. Ohlhorst (2014) explains that company, BitGlass, developed a proxy-based system using SAML to authenticate, secure access and log activity through the cloud. This showed that SAML can be used to detect suspicious activity and the companies would then wipe all information affecting a user’s data if they were breached.

Active Defence Measures

Active defence measures are based on the idea that instead of waiting for a security breach, the user takes the proactive measure to go after the breacher. Out of all the securities it is the most controversial due to the ability of some participants having to be involved in illegal activities to combat cybercrimes (Writers 2021). A few that are known are counterintelligence gathering, sink holing, honeypots and retaliatory hacking (Writers 2021). The most recent and more experimental measure is MonsterMind developed by the NSA (Zetter 2014). According to Edward Snowden this automated program, set like an AI, would use algorithms to search metadata, identify then block malicious network traffic (Zetter 2014). This same program could shut the servers as well within the attacks.

Early Warning Systems

Early warning systems is the most recent innovation which is in the early stages and a glimpse of what is to come. Utilising machine learning and data mining techniques, an algorithm that can predict which web servers are likely to become victim to malware or breach is being developed (Writers 2021). The algorithm considers similar characteristics of vulnerable websites such as software, traffic, filesystem structure and webpage structure. Christin & Soska (2014) applied this algorithm and predicted that 66% of websites turned up potential for being hacked with only 17% as false positives. Other more newer technologies like FIDeS have made the technology more AI like in nature where it can now detect from both local area networks and in wide area networks (LIFARS 2020).

Impact on Society

As society is becoming more technologically dependent, the slew of cybercrimes and attacks will not reduce without the continuous development of the aforementioned technologies. According to Tunggal (2021) these developments will continue to give companies and users the ability to protect themselves from theft of their intellectual property, and/or information. Ultimately reducing economic costs on top of protecting the reputations of companies and individuals by ensuring this sensitive data is not shared or improperly used. Whilst being very positive in nature some issues were brought forward in the World Economic Forum (2020) about the posing risks in the increasing nature of cybersecurity. These risks according to the World Economic Forum (2020) were:

- Risk to the global economy. It is noted as one of the most systemic issues due to the collective spending involved to maintain and develop. This is due to the major technology trends and experts have questioned whether it would remain sustainable due to these factors.

- Risk to the operational capabilities and design of these securities. As they become more complex in how they manage data they essentially require high level of computing capabilities to simply run.
- Risk to the community management and leadership. The need for industry and government education, and leadership poses a potential issue as it requires users to become more involved or aware of the process. They would then need to cooperate with policy makers to consider responsibilities.

Overall cybersecurity is an important feature to have it does pose risk due to the highly volatile nature of the technology and what is established to be protecting.

Personal effect

Personally, this would be very positive regarding daily life. Increased security measure protecting my interests as well as my family and friends is beneficial to us all. I believe the most difficult issue is that with the increasing security, the more intricate designs will have to be utilized for just simple amount of data for i.e., using multiple keychains to access personal data or multiple checks to ensure that activity is not suspicious. This will require more paying attention to systems and certain securities behind them so for more elderly members this may prove to be more difficult. Overall, though for my family as whole this will help to protect assets and our digital footprint to ensure that cyberattacks are not committed that could lead to potential harms.