Cyber-attacks

Introduction

Assume that you have been appointed to a task force of 5 or 6 computing professionals within your organization. You have been asked to examine the current issue outlined in the article below. Your team has not been asked to make specific recommendations to solve the problem. Rather, you have been asked to make recommendations that will help the Government decide what next steps they should take.

Prompts

1. What is/are the problem/problems here? Is there an underlying fundamental problem?
2. Who are the major stakeholders and what are their perspectives?
3. What are the major ethical, legal, and security aspects associated with the problem?
4. What are the intended and unintended consequences of existing computing solutions? Consider the consequences on individuals, organizations and society within local and global contexts.
5. What recommendations do you propose that may lead to potential solutions?

Cyber-attacks in the UAE increased by 400% in 2014, despite strict penalties on cyber criminals such as fines up to 3 million AED. According to cyber security company Norse, the UAE ranks as the second most targeted country. Cyber-attacks in the GCC region are costing approximately 3.67 billion AED per year, and it's believed many more cases are unreported as companies and banks fear damages and loss of confidence if they make the attack public. Also known as a computer network attack, cyber-attacks alter computer code, logic or data with disruptive consequences. Cyber-attacks cover a wide range of crimes, such as fraud, identity theft, credit card theft, spamming, phishing, and data theft.

The use of technology for banking, the amount of investments in the UAE and the free zones in Dubai have increased the attack surface of the UAE. The UAE is implementing the use of technology across all areas of resident's lives, from paying traffic fines to registering for an ID card, which makes it more digitally visible. Most attacks are on the financial sector, including ATM and internet banking, claims the Ministry of Interior. The second sector most targeted is the oil and gas industry, which has also digitised information and processes. Consumers in the UAE also rank 4th for experiencing a new type of attack called ransomware, whereby files are held ransom and the consumer pays to have them recovered. Symantec claims the average ransom paid increased to 2491 AED in 2016, and this type of attack rose to 44%. Security software is not enough to protect users, and with an estimated 85% of UAE society connected to

the internet, and as a global leader in smartphone penetration, the UAE is a lucrative market. The potential for attacks is predicted to grow in the UAE with the development of the knowledge economy and smarter cities.

Globally, 2016 saw some of the largest cyber-attacks to date, and this trend is expected to continue. In one of the biggest cyber-attacks ever, Chinese Google experienced Operation Aurora which stole intellectual property. There was also an 11 hour attack against an American DNS service which effected more than one billion users, disrupting service to websites such as Amazon and Netflix. Yahoo reported two major data thefts, compromising over a billion accounts with leaked personal information, 60 million dropbox users were hacked and 100 million LinkedIn passwords were compromised. While cyber-attacks can cause inconvenience and chaos, loss of revenue and data, there can be more serious implications.

Cyber technology can take over drones, or smart devices, and use them as explosive devices because anything with an IP address can be infected or attacked. In 2015 Ukraine suffered a cyber-attack which left 225,000 people without electricity. The attackers remotely accessed the industrial control systems and shut down the power supply from 30 stations. Earlier, in 2010, the Stuxnet worm attacked over 15 Iranian nuclear facilities and was believed to have been introduced to the system via USB. More recently in 2018, the US Computer Emergency Readiness Team warned numerous European countries that their power plants had been hacked by suspected Russian operatives. While not yet a full cyber war, there are clearly cyber incursions underway between countries like Russia, China, North Korea, and the US. Other countries like the UAE also need to be prepared.

The UAE has teamed up with America to strengthen their abilities against cyber-attacks, and there is an increasing emphasis on security. A recent Cyber Crime Conference in Abu Dhabi was attended by police, university professors, law and IT students, legal advisors, judges and security agents, and the budget for fighting cyber-attacks is growing massively. Experts say the global pool of IT security experts is shrinking, and so the UAE is investing in training its own security professionals. Security company DarkMatter is establishing a cyber security academy in the UAE to create more local talent. A special prosecution department, the Federal Public

Prosecution for Information Technology Crime, was started in 2017 to deal with criminal case specific to information technology. The International Cyber Crimes Conference in the UAE identified the importance of upgrading legal frameworks and issuing more regulations to cover cross border crimes and e-police patrolling the Internet. “There are now more devices than there are humans on the planet, so it is getting easier for anyone…… to buy a botnet army to launch attacks”, said Eric Eifert from DarkMatter.

Bibliography

Altaher, N. (2016, May 12). *UAE a Target of 5% of Global Cyber-Attacks*. Retrieved from Gulf News: http://gulfnews.com/news/uae/crime/uae-a-target-of-5-per-cent-of-global-cyber-attacks-1.1826610

Arabian Business. (2015, January 30). *UAE teams up with US to fight cyber crime*. Retrieved from Arabian Business: http://www.arabianbusiness.com/uae-teams-up-with-us-fight-cyber-crime-580116.html

Keating, D. (2018). *European Power Plants Brace For Russian Hack Attacks*. Retrieved from Forbes: https://www.forbes.com/sites/davekeating/2018/03/22/european-power-plants-brace-for-russian-hack-attacks/#3c3da8da7226

Masudi, F. (2016, July 21). *Ordinary residents are majority of ransomware victims*. Retrieved from Gulf News : http://gulfnews.com/news/uae/crime/ordinary-residents-are-majority-of-ransomware-victims-1.1866436

Rhea Group . (2016, August 19). *The Three Biggest Cyber-Attacks*. Retrieved from Rhea Group : http://www.rheagroup.com/three-biggest-cyber-attacks-2016/

WAM. (2017). *This is how UAE will deal with cybercrimes*. Retrieved from the Khaleej Times: https://www.khaleejtimes.com/news/crime/this-is-how-uae-will-deal-with-cybercrimes