CET324 – Advanced Cyber Security Assignment 1

Part 1

Introduction

The cybersecurity landscape is constantly changing for both individuals and companies as companies and individuals become more tech savvy and are more prepared for traditional forms of cybersecurity such as phishing emails. This report will highlight some of the most common forms of attacks, how likely they are to occur, how they affect individuals and organisations, where the threats are likely to come from and what the impact could be and the consequences.

Phishing/spoofing attacks

Phishing attacks are attacks aimed at getting confidential information be that personal information, or login information for online banking. This is done be pretending to be a legitimate company, the most common is pretending to be a bank and asking the user to log into their account and providing them to a link that looks like the proper bank website. The user will enter their information and that will be given to the criminals. These types of attacks are very common, according to the Wombat Security Technologies report for 2015 (Wombatsecurity.com, 2015) 85% of surveyed business said they suffered at least one phishing attack. Spear phishing, which is a more targeted version of phishing saw a 22% rise from 2014 to 67%. This is a threat against both individuals and organisations as was demonstrated in 2016 when a group known as threat group 4127 target Hillary Clinton's emails using phishing emails, using a fake google login domain. The same group targeted over 1800 google accounts using the same system. (Secureworks.com, 2016). The biggest impact that comes from phishing for a company is that the attackers have access to login information which they may use to break into servers and steal information to sell later, if this occurs it can lead to less consumer confidence in the organisation to protect their data. As for the individual the results of phishing can be huge, most of the time these attacks target banking information. The consequences of that banking information being stolen could result in identity theft as well as a huge hit to your credit score. These types of attacks mainly come from Eastern European countries and Russia.

Ransomware

Ransomware is a form of malware which either threatens to leak the information stored on a computer or block access to it unless a demand is reached. The demand normally comes in the form of a bitcoin transfer. The way ransomware works is that it targets a computer's files and encrypts them, advanced versions of ransomware encrypt certain files such as word documents and PDFs with a higher level of encryption as they're more likely to be sensitive files the victim will want back and are harder to crack. Normally if the ransom is paid the attacker will release a command to the ransomware to decrypt the files, however more recently either due to bad coding or attackers not caring, ransomware has not been unlocking even if the ransom is paid. Ransomware is increasingly becoming more and more common especially against organisations. Globally 40% of business fell victim to ransomware attacks. In the UK that number was 54%. (Hern, 2017) The biggest and most recent example is WannaCry. The ransomware was fairly unique as normally a user has to download the ransomware and it'll infect the machine it is downloaded to, however WannaCry also was a worm, which allowed itself to spread to every computer on a network. In the Uk the NHS was hit very badly as a "total of 48 National Health trusts were hit" (BBC News, 2017). The impact of ransomware on both individuals and organisations is the potential loss or leak of sensitive information. The consequences of this are broad but most notably people will feel less confident in

an organisation that falls victim to these sorts of attacks. As for the average person the loss of potentially sentimental data such as family photos has a profound emotional impact. These types of attacks mainly come from former soviet states. Although it has been alleged that North Korea is using ransomware to fund it's military.

DDoS attacks

Distributed Denial-of-Service attacks or DDoS attacks are attacks where a huge amount of traffic is sent to the victim's servers from multiple places, making blocking them difficult. The objective of this is to take the website or online service offline from overloading the servers. This is normally accomplished by using a tool called a botnet. A botnet are a bunch of infect computers or routers which are controlled but not owned by one person. When they want to do a DDoS attack they command the botnet to keep accessing the online service. Most of the time people do not realise their computer or router is part of a botnet, which make fighting DDoS attacks difficult as you can't ban the systems responsible as they're often hard to pick out of the legitimate traffic trying to access the server. Most websites now have DDoS protection such as CloudFlare, this works by limiting the access to a server once traffic reaches a certain value. While this slows down the service to the server, it normally keeps them operational. DDoS attacks are becoming more and more common, there was a "125.36% increase in total DDoS attacks" (Akamai, 2016) from Q1 2015 to Q1 2016 and in the same time period there was a "137.5% increase in attacks > 100 Gbps: 19 vs. 8" (Akamai, 2016). This shows that these attacks are getting worse as so called "mega attacks" are being targeted at bigger companies. On Christmas Day in 2014 both Microsoft and Sony suffered "mega attacks" against their online gaming services. (Kiss, 2017) DDoS attacks are not commonly target at individuals, although small scale tools were used by online gamers, which are known as "lag switches" which would do small DDoS attacks against opponents to make them have connection issues. Most DDoS attacks are targeted at companies and the impact can be high for these attacks. They are especially damaging for online retailers as during the outages caused by DDoS attacks revenue is lost. These attacks come from all over the world, with hacking groups all over the world using DDoS attacks to achieve their aims.

Conclusion

This report has highlighted the 3 most common attacks that organisations and individuals face. Although there are many other different threats such as traditional hacking techniques, insider threats, automated scanners, worms/viruses and adware. It has also outlined what they are, where they come from, how likely they are to happen, and the likely impact and consequences of these attacks.

Part 2

Introduction

The idea of opening a cyber security clinic in Sunderland is a good idea and I will explore the idea in this essay. This essay borrows heavily from the Tutorial from Session 9 as well as the lecture slides. I will go into detail first bout the benefits of opening such a clinic, the activities that might be undertaken in the clinic, the possible concerns about the establishing of the service and issues concerning liability and any legal and/or professional concerns.

Benefits of a clinic

Students would be one of the main beneficiaries of opening a cybersecurity clinic in the university. The benefits to students who have cybersecurity modules would be very high as the research into the aspects of cybersecurity would allow for their education to be very up to date. As well as this, students would also be able to do work experience at the clinic which would in turn help them to get better jobs. The clinic will also be able to help students with their own cybersecurity advising them on best practices as well as helping students to recover if they ever suffer from a cyber-attack. Another benefit for students, especially for students wanting to pursue a career in cybersecurity would be to allow them to do dissertations on cybersecurity issues.

Employees of the university will benefit as well as the clinic will be able to help them with their personal cybersecurity and cybersecurity at work. Advising them on best practices for in the office and outside of the office, as well as helping them recover if they suffer from a cyberattack. It will greatly benefit the IT staff at the university as they clinic will be able to advise them and to help them with their jobs, making their jobs easier. Faculty of Computer Science lectures will also greatly benefit from this clinic as it will allow them to easily do research on topics related to cybersecurity and cyberattacks, as well as allowing them to have access to the latest information and strategies for their teaching materials.

The university would benefit hugely from the clinic. The main way being that the university would no longer have to outsource for its cybersecurity as the clinic would be cheaper and just as effective, plus having the clinic on campus would mean the response times to a cyberattack would be much quicker, and the locality of the clinic would allow for easy meetings with the Dean and university management. As well as those the clinic would raise the profile of the university as it would be a centre of cybersecurity, as well as providing a big draw for students to come study cybersecurity at Sunderland university by increasing the rankings for all computing related courses.

Individuals and organisations outside of the university would be greatly benefited by the clinic as they would have somewhere to go to get advice on things such as how to set cybersecurity and how to respond to attacks. As well as that they could send employees to receive training there so that they could be Data Protection Officers for the GDPR bill coming in, in May 2018.

Activities that might be undertaken

Research security vulnerabilities would be one the main activities undertaken by the clinic, this research would be primarily aimed at defences against current and up and coming threats such as worm based ransomware like WannaCry. The research would be done by PHD students, lecturers and dedicated researchers, and their work published, and solutions monetised.

Handle security incidents would be another of the main activities of the clinic. This wold consist of the clinic helping out victims of cyberattacks, whether that might be trying to decrypt a piece of ransomware or providing assistance on analysis of security breaches to see what was affected and

what steps to implement to make sure that the incident does not occur again. As well as potentially working with the police and other government agencies to try and track down the perpetrators of the attack.

Announce security alerts to the public and business is a very important activity for the clinic to do as it has to make sure that the public and especially business are aware of trends in threats and very wide threats such as a particularly good phishing campaign for example so that the public and business can make sure they're aware of it and to avoid it. The most important part of this is to make sure that these alerts and understandable and accessible by everyone, so making sure to avoid technical jargon is of paramount importance, and that it is not buried somewhere online. Most likely an email list would be used to alert people who wished to be alerted, as well as trying to get pieces published in the local news to make as many people aware as possible.

Another important action that would be undertaken would be to provide security solutions to organisations, this could be done through propriety software or through bought software. The clinic could provide the setup and management of the software for the organisations. As well as software, doing things such as risk analysis on an organisations' systems to make sure that the correct security solutions are being presented as well as making sure that the organisations' physical security is up to scratch as well to avoid social engineering and insider threats.

Provide advice to students to make sure that they are prepared to deal with cyberattacks by making sure they have an anti-virus as well as anti-malware software, and making sure their definitions are up to date and that at least weekly automated scans are setup and that they will be done every week to make sure that the computer is safe from generic cyberthreats.

Operate as a consultancy for organisations, making sure the organisations see cybersecurity as important and talk through the ways to prevent cyberattacks in the first place such as having an internal network and using the principal of least privilege to make sure that internal threats are prevented. Making sure that the organisation is provided with monthly security reports on their own security and current threats they need to be worried about.

Using the clinic as an educational resource would be a major activity as the clinic is part of the university, and as such not only students but staff of the university would be to access the clinic as a educational resource. Maybe yearly course for both staff and students on the basics of cybersecurity and using it to support student dissertation projects and PHDs.

As a training facility the clinic would prove invaluable especially with the GDPR coming in 2018, companies will need Data Protection Officers trained and ready to go, as well as providing the service to organizations and letting them outsource it to the clinic, the clinic would also offer training courses to allow organisations to send someone to be trained.

Concerns about establishing a service

In terms of physical space there are 3 important things to consider, size, environment and storage facilities. First of all size, size is important because you can't have a place that's too small or one that's too big. With both university campus' being so filled up it is likely the clinic would need to have a new building to call home. As for environment, the place has to have proper ventilation and air conditioning as well as backup systems and UPSs so as to make sure that if there is a power

failure the computer are protected. Last but not least is storage facilities, the storage facilities need to make sure that they are fireproof, waterproof and electronic interference is kept to a minimum.

Security is paramount to the running of a cybersecurity clinic. The first part of the security we'll focus on is physical security. This will take the form of keeping the work area to authorised persons only, and the way you'd be able to access that is to use 2 factor authentication. As well as this, keeping the servers networked to the lab itself only, this makes sure that the risk of an external attack is reduced significantly. The other is the software security. This is pretty simple stuff such as access controls, firewalls, anti-virus, intruder detection. This helps to make sure that if something bad got into the system, at least something would top it or sounds the alarm.

The cost of the clinic would be high especially the set-up cost from buying all the hardware and software as well as hiring people, so investment would need to be secured, most likely from the university or from other generous patrons.

Issues concerning liability and any legal and / or professional concerns

As of right now, the Data Protection Act 1998 would be the main legal liability, although when the General Data Protection Regulation comes into force in May 2018 that will be the sole legal liability to protect the data that we have, as we could be fined 4% of our global revenue. So, it is important that we take steps to protect the data that we use. Since we will be handling and processing data we will need a Data Protection Officer to make sure that our data is protected.

In terms of business using us as their cybersecurity team or cybersecurity advisors, we need to make sure that these companies that we interact with sign a contract that shifts all of the blame off of us and onto them in the event of a breach of their cybersecurity.

Conclusion

In conclusion the benefits for students, employees of the university, the university and Individuals and organisations outside of the university would benefit greatly from Sunderland having a cyber security clinic. The main benefits are clearly to education, in raising the standards for the computing courses offered by the university but also helping students to gain that valuable job experience. As well as that, this report has outlined the activities that the clinic would do and explained them. As you can see from the above report the list is extensive. This is to make sure that the operational cost of the clinic is met with the amount of activity needed to make sure that the clinic is successful. The cost of the clinic will not be cheap at least initially but once the money has gone on hardware and software, the only running costs will be salary and utilities, so it will get cheaper to run in the long term.

Part 3

Introduction

Cybersecurity is important to both individuals and organisations, and there are steps that both can do to help prevent cyber-attacks and to recover and learn from cyber-attacks.

Risk Analysis

Risk analysis is all about determining what risks and the chance of those risks happening, and working out what the risk to reward is in terms of security features, this is both helpful for organisation and individuals, but more so for organisations as they're at more risk of cyber-attacks, however an individual should also perform a risk analysis as it could help identify potential flaws in their security. The cybersecurity actions that risk analysis provides is to identify key data or systems, and what the specific risks to them are and how likely they are, as well as working out what cybersecurity measures need to be taken to defend the data or system and how cost effective it is to implement these security measures. For example, you are not going to implement DDoS protection on a system which has say a 1% chance to suffer from one. This helps the organisation or the individual to avoid getting unnecessary protection. The effectiveness of a risk analysis is entirely dependent on two things, how it is conducted and if it is for an organisation or individual. For an organisation they cannot do a high-level overview, it would need to be a low-level analysis to be effective. For an individual they can do a low-level analysis, but it is unnecessary to do so. The cost of performing a risk analysis is generally low as it only requires an organisation or individual to perform an analysis on their systems, something they should be familiar with. Not only that but risk analyses actual save money in the long term by making sure that money spent on cyber security goes where it is needed.

Meeting Government Requirements

While this does not affect individuals in terms of what they can do to protect themselves, meting government requirements does affect organisations. There is currently one piece of legislation that governs cyber security which is the Data Protection Act 1998 (DPA), business that use data have adhere to strict regulations on how they can use the data and follow security principles to protect the data. In May 2018 the UK will have a new piece of security regulation known as the General Data Protection Regulation (GDPR). Both the DPA and the GDPR make sure that organisations need to protect the data they use. As discussed in the Session 10 tutorial and the Session 4 tutorial the GDPR will have a massive impact on the way originations conduct their cyber security. For example, data protection will have to be by design and by default meaning that systems will have to be designed early on with data protection in mind, combined with the fact an organisation will be fined up to a maximum of 4% of their annual turnover, will make sure that organisations take government regulation seriously, and make sure their cyber security is up to scratch. The current regulation, the DPA, is rather lacking in effectiveness, as while it works to a certain extent, its age is starting to show, and as such is becoming less effective. Plus, with its mediocre maximum fine of £500,000 is not very effective in making business think about cyber security. However, the new GDPR will be very effective in making organisations take cyber security seriously due to the massive fines that they will incur if they do not protect data effectively. The cost to an organisation to implement

government regulation can be quite high however from May 2018 across all the EU it will be costlier for business to not implement good cyber security as 4% of their global revenue is a lot more than what it would cost to make sure data is protected.

Other steps before an attack

There are some other steps to take before an attack, these revolve around 2 principles, the principle of least privilege which is designed to stop an insider attack as it only allows a user access to the data they need to complete their job. The other principle, the principle of separation of risk builds upon least privilege, whereby you keep different systems separate from one another to stop the risk of a cascade. This can be as simple as keeping personnel records and accounting on a different server. The idea of confidentiality is what links those two principles together as you need to keep information private/secret to those who don't need to see it, and you can achieve this through a variety of methods but one of the easiest is to keep sensitive information off of publicly available systems and networks. Integrity is a step which involves making sure that while people can see the data only those with the correct responsibilities can edit the data and that all of these changes are properly recorded.

Steps after an attack

As has been discussed above there are multiple steps that can be done before an attack but what do you do after. Well you must first detect that there has been a security breach and work out what has been affected, this can be done through software such as access control and intruder detection, both in parallel will allow you to be alerted in case of a breach in security and you will be able to find what was altered or taken, and that is the first step in response, to find out what damage has been done. The second step is to alert the higher management of the organisation or in an individual's case alert the police. Then for the 3rd step is to identify the breach and repair it, followed by for an organisation notifying people if their data has been compromised. The penultimate response is to try and restore the data back to the way it was if it was altered or deleted, the final response is to evaluate your cyber security and make the necessary changes.

Conclusion

In conclusion, there are a number of steps that an individual and an organisation can take before an attack and this is the best time to take those steps as once there is a breach it is too late to implement these steps until the breach is resolved and by that time the organisation could be in ruins due to the damage done. However after an attack you can still implement steps to make sure the same attack doesn't happen again and to make sure that another attack doesn't happen in the future.

References

Secureworks.com. (2016). Threat Group-4127 Targets Google Accounts. [online] Available at: https://www.secureworks.com/research/threat-group-4127-targets-google-accounts [Accessed 8 Nov. 2017].

Wombatsecurity.com. (2015). New Report on the State of Phishing Attacks from Wombat Security Shows Significant Increases Year over Year | Wombat Security. [online] Available at: https://www.wombatsecurity.com/press-releases/new-report-state-of-phishing-attacks [Accessed 8 Nov. 2017].

Hern, A. (2017). Ransomware threat on the rise as 'almost 40% of businesses attacked'. The Guardian. [online] Available at: https://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked [Accessed 8 Nov. 2017].

BBC News. (2017). Cyber-attack 'unprecedented' in scale. [online] Available at: http://www.bbc.co.uk/news/world-europe-39907965 [Accessed 8 Nov. 2017].

Akamai (2016). akamai's [state of the internet] / security / Q1 2016. [online] Akamai, p.6. Available at: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q1-2016-state-of-the-internet-security-report.pdf [Accessed 8 Nov. 2017].

Kiss, J. (2017). Xbox live and Playstation attack: Christmas ruined for millions of gamers. The Guardian. [online] Available at: https://www.theguardian.com/technology/2014/dec/26/xbox-live-and-psn-attack-christmas-ruined-for-millions-of-gamers [Accessed 8 Nov. 2017].