International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 1 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT19519

Cyber Security, Challenges, Some Practical Solutions

[1]Y. V. Sai Bharadwaj, [2]Sai Bhageerath Y.V, [3]Prof. Y.V.S.S.S.V. Prasada Rao
[1]Central University of Hyderabad, Hyderabad, Telangana, India
[2]National Institute of Technology, Warangal, Hanamkonda, Telangana, India
[3]Pattabhipuram, Guntur. Andhra Pradesh, India

ABSTRACT

Cybercrime continues to surge without a slowdown in sight. The cyber security threat continues to worsen. In the first half of 2018, the number of cyber breaches soared over 140% from a year earlier, leading to 33 billion compromised data records worldwide. Cyber Security news such as Marriott hack in Nov 2018 is dominating headlines and becoming a serious headache for business leaders. Malicious outsiders sparked more than half of the 944 breaches and accounted for roughly 80% of stolen, compromised or lost records. Identity theft continues to lead data breach types, but financial access incidents are escalating in severity as well. The United States continues to be the favorite target, and data breaches at major US enterprises continue to grab the headlines. In 2018, the most notable breaches have occurred at Adidas, FedEx, Jason's Deli, Macy's, Under Armour, Nordstrom's and the most popular Facebook. [1].

Keywords : Cyber Security, Quantum Computing, Crypto-Agility, Phishing, Cyber Insurance, Phishing attack, JDLR, Emotional Blackmail, CCO, TalkTalk Data Breach

I. INTRODUCTION

Cybercrime continues to surge without a slowdown in sight. The cyber security threat continues to worsen. In the first half of 2018, the number of cyber breaches soared over 140% from a year earlier, leading to 33 billion compromised data records worldwide. Cyber Security news such as Marriott hack in Nov 2018 is dominating headlines and becoming a serious headache for business leaders. Malicious outsiders sparked more than half of the 944 breaches and accounted for roughly 80% of stolen, compromised or lost records. Identity theft continues to lead data breach types, but financial access incidents are escalating in severity as well. The United States continues to be the favorite target, and data breaches at major US enterprises continue to grab the headlines. In 2018, the most notable breaches have occurred at Adidas, FedEx, Jason's Deli, Macy's, Under Armour, Nordstrom's and the most popular Facebook. [1].

II. Cyber security in small and medium sized companies

2.1. Issue :

Cyber security in small and medium-sized companies is a big issue, but businesses can take steps to protect themselves. The issue of cyber security in small and medium-sized companies is becoming vital. [2]

As for cyber security in small and medium-sized companies, many are realising that they are viewed as attractive a target as the larger companies. Cisco's 2018 SMB Cyber Security Report found that 53% of mid-market companies in 26 countries experienced a breach. For these companies, the top security concerns are targeted phishing attacks against employees, advanced persistent threats, ransom ware, denial-of-service attacks and the proliferation of employees allowed to use their own mobile devices.

Malware of all types is a huge problem. It is becoming more difficult to combat as cyber-attackers get more adept at developing software that can evade traditional detection and employ more sophisticated malware. For small and medium businesses, one breach often puts a victim out of business. That's because 54% of all cyber-attacks cause financial damages exceeding $500,000, the 2018 Cisco SMB cyber security report shows. That price tag along with a damaged reputation are hard to survive. If they do survive, they still face significant system downtime that averaged eight hours or more in the last year. Further, such companies often lack the IT talent, budget and technologies to prevent, uncover and respond to an attack.

2.2. Prevention of Cyber Theft :

Unsurprisingly, there is no easy solution – and none is likely within the near future – to prevent data breaches. But all businesses, especially small and medium sized companies can become better prepared and more adept at protecting against cyber-crime.

Here are five actions concerning cyber security in small and medium-sized companies that can be taken to become more security-conscious:

1. Conduct a security audit. Learn how secure your network and other security systems are, where vulnerabilities exist and how to resolve them. If you consider cybersecurity insurance — currently the fastest-growing insurance — or have coverage from a business insurer, the insurer can usually refer you to resources to assist in the audit.
2. Ensure you have a proper backup system. And make sure it is easy to access in case you need to restore one piece of the system rather than the entire system. Enterprise-level cloud systems can help.
3. Examine all the entry points into your system and consider where they are vulnerable. These include all your workstations, communications and mobile devices as well as employee access cards, the internet and cameras.
4. Assess your system threats. These include client lists, passwords, data logs, backups and emails, and anyone who specifically has access to the system, including customers and vendors.
5. Put a prevention system in place to defend against intruders. Put yourself in the place of the cyber attacker and consider the possible ways the attacker could access your system and steal your data. If your internal IT staff isn't experienced enough to handle, entrust a third-party firm, because the prevention system must cover physical and digital security.

III. Quantum Cryptography: The next-generation of secure data transmission

3.1. Issue:

Quantum Computing will render much of today's encryption unsafe. But Quantum Cryptography could be the solution. China has recently successfully tested – for the first time – its quantum communications system, which cannot be hacked. [3].

3.2. How does quantum cryptography work ?.

Quantum cryptography provides a secure method for generating and distributing secret keys between two parties via an optical network. This is achieved by capitalising on the inherent unpredictability in the state of particles – such as photons or electron – to generate the random numbers needed for cryptographic applications. The technology then harnesses this to create and share a secret digital key that can be used to encrypt or authenticate information via streams of encoded single photons, which are sent through an optical communication network.

3.3. The arrival of quantum cryptography :

The arrival of quantum computing will ultimately render much of today's encryption unsafe. The current consensus that public key encryption is an essential part of data security is starting to be questioned in the face of new attack strategies – which is subsequently driving uptake of robust quantum cryptography solutions and services to deliver better data security. As a result, the global quantum cryptography market is forecast to grow from USD 285.7 Million in 2017 to USD 943.7 Million by 2022, a Compound Annual Growth Rate (CAGR) of 27 per cent according to Research and Markets. In reality, however, as things stand today quantum cryptography is not quite so close to mainstream fruition.

IV. Crypto-agility: the key to ensuring long term website security

4.1. Issue :

In the age of the internet, you simply cannot afford to do business without being online, and keeping your website secure should be a top priority [4].

4.2. Crypto-agility to the rescue :

This is why organisations need crypto-agility – i.e. the ability to manage machine identities in real-time. Crypto-agility enables businesses to quickly identify and replace certificates in bulk when security events or business needs call for it. Currently, many organisations take days or even weeks to find and replace certificates, which isn't conducive to ensuring security. By automating the process, this process can be resolved at the click of a button. Crypto-agility has never been more important to ensure businesses can confidently protect themselves and their customers from hackers. This is why organisations must invest in a credible technology to automate the tracking of certificates; it is no longer feasible to do this manually, there are simply too many certificates to track. Companies focusing too much on protecting usernames and passwords and not enough on machine identities.

4.3. A future-proof solution :

Google's decision to distrust Symantec certificates doesn't need to be the end of the world. If companies are able to manage all their machine identities centrally and automate the process, it will enable crypto-agility and ensure they can migrate quickly when a flaw or vulnerability is discovered. By doing so, companies can insulate themselves against the volatility of the CA market, protect their reputation and ensure business continuity for online services.

V. What is phishing ?

The word 'phishing' was invented as a homophone of 'fishing' as it involves creating a bait to lure victims. Typically it involves an email; although sometimes a telephone call – called Vishing – or a text – called Smishing. These emails are often credible enough to deceive the recipient into clicking on a link which could then release malware – viruses, worms, Trojans or bots – onto the recipient's computer or take the victim to a fake website.

5.1. How to protect against phishing :

The following are the tips against phishing.

5.1.1. Never, ever follow suspect links

There is no 100% guaranteed way to detect phishing but, if there is the slightest suspicion that the email may be fraudulent, do not click on any links it contains. Always enter the sender's website address (not the link in the email) directly into your browser.

5.1.2. Check out the sender

Be warned if the part after the 'at' sign @ in an email address doesn't match the purported sender; for example, if 'PayPal' sends you an email from paypal@emails.com or the URL is misspelled as www.paypa1.com or something similar. This is a (fake) website owned by a cyber squatter. Some of the most well-known companies in the world have website impersonators including Facebook, Google, DropBox and PayPal.

5.1.3. Don't give in to emotional blackmail

Phishing mails almost always contain the same kind of content and requests. Sometimes, they ask you to update your user account or password. But sometimes they use psychology to get you to react: the notification of a big lottery win, an offer to take part in a once-in-a-lifetime business opportunity or, an appeal for a donation to a charity.

5.1.4. Banks never want to know this

There are some things that your bank will never ever ask you. They don't want your passwords or PINs to be sent by e-mail or text; they don't want you to authorise the transfer of funds to a new account; and they don't want you to meet a bank representative at your home to collect cash, bank cards or anything else.

5.1.5. Beware of opening attachments

If attachments with unknown file extensions (or PDF files) suddenly appear as an e-mail attachment, it is a clear indication that something is wrong – especially if you haven't had any previous dealings with the sender.

5.1.6. Personal salutation

Most companies address their customers by name. But if the name is missing, misspelt or if there is no name at all and it just says something like 'Hey' or 'Dear Customer', it could be an indication that this is a fake email.

5.1.7. Trust is good but control is better

By regularly checking your bank statements, you can mitigate any potentially serious consequences of a phishing attack. Any suspicious or unknown transactions should be reported directly to the bank or credit card company immediately.

5.1.8. Keep yourself up-to-date on current scams

Take the time to read up regularly on ways to protect your digital safety. If you hear that a service provider has been hacked, be sure to follow their instructions and change your password.

5.1.9. Only use secure websites

When conducting online transactions, go directly to the website. If the special offer is genuine, it will be available on the website. Look for a sign that the site is secure, such as a white padlock icon on the browser's status bar or a "https" URL (where the "s" stands for "secure").

5.1.10. Protect your computer with a firewall, spam filters, anti-virus and anti-spyware software.

Do some research to ensure you are getting the most up-to-date software, and update them all regularly to ensure that you are blocking new viruses and spyware.

5.1.11. Click in haste, repent at leisure

Many phishing e-mails put pressure on you to act quickly or else, they threaten, something bad will happen or you will miss out on something very important. A 'bank' might warn you that your account will be closed unless you act quickly; or a company might tell you that you have won a major cash prize, but only if you can claim it in the next 24 hours. Don't act in haste. Take your time to satisfy yourself that the message is genuine.

5.1.12. Genuine messages don't make threats

Although most phishing scams involve trying to trick or persuade people into handing over sensitive information, some fraudsters use fear and intimidation to scare their victims. For example, threatening to send embarrassing videos or photos to contacts unless a ransom is paid. Try not to react immediately to an email take a few minutes to calm down and think rationally. Why would this person be emailing you, specifically about this, all of a sudden?.

5.2. The JDLR rule :

Criminals are now able to put together professional-looking messages and web pages which can trick even the most discerning person into giving away personal information when they are tired, busy or stressed. Check your privacy settings on popular social networks to restrict how much personal information you are making public and above all, follow the JDLR rule. If it 'Just Doesn't Look Right', then it probably isn't. [5].

VI. Cyber security trends in 2019

The following are the cyber security trends and issues (more stringent regulation, creations of new roles etc.,) the world can expect in 2019: [6].

6.1. Cyber security regulations improvement

We need to see a continuing improvement in the relevant regulations as apply to cyber security. The dynamic and fast-moving nature of cyber security outpaces regulation which is far too slow and clumsy to be of any benefit and might actually hinder security by building a culture of compliance with regulations and a false sense of security against enemies who are agile, motivated, and clever.

6.2. Data theft turning into data manipulation

We can expect to see attackers changing their methodology from pure data theft and website hacking to attacking data integrity itself. This type of attack, in comparison to a straightforward theft of data, will serve to cause long-term, reputational damage to individuals or groups by getting people to question the integrity of the data in question.

6.3. Demand will continue to rise for security skills

A global shortage of cyber security skills in the workplace arguably makes organisations more desirable targets for hacking. Demand for expertise will rise as companies realise that their current IS strategy is not sufficient. Also, with companies increasingly insourcing their security needs, internal training and skills growth has to continue to accelerate. Tailored training programmes are crucial.

6.4. Cyber security and Internet of Things (IoT)

'Secure by design' will garner much copy, but probably will not deliver until 2019 or beyond. We'll have to wait and see with this, as connected devices are increasing in circulation by the day, and perhaps it is only a matter of time before the security vulnerabilities are exposed — could there be a repeat of the Mirai Botnet in 2019?. Indeed, the next generation of AI-powered attacks will be crafty enough to emulate the behaviours of specific users to fool even skilled security personnel.This might include the ability to craft complex and bespoke phishing campaigns that will successfully fool even the most threat-conscious among us.

6.5. Attackers will continue to target consumer devices

Ransomware is a recognised problem for companies of all shapes and sizes, epitomised by the large scale WannaCry attack that decimated the UK's National Health Service (NHS) and organisations around the world. In 2019 and beyond, will we start to see consumers being targeted across a range of connected objects? This is a likely scenario, with examples coming out of child predators targeting IoT devices in toys (designed for children). Attackers might even target the smart TV in your house via a ransomware attack that would require you to pay a fee to unlock it.

6.6. Attackers will become bolder, more commercial less traceable

Hackers will look to become more organised and more commercialised, perhaps even having their own call centres – something already seen with fraudulent dating sites. They will look to base themselves in countries where cybercrime is barely regarded as a crime and thereby placing themselves outside their victims' police jurisdictions.

6.7. Attackers will get smarter

Attackers capability to write bespoke targeted code will continue to improve faster than the defenders ability to counter or get ahead of it.They will continue to exploit the Dark Web, a small portion of the Deep Web, in order to successfully hide and to communicate with other criminals.

6.8. Breaches will get more complicated and harder to beat

Cybercriminals will look to grow their malicious activities using malicious code in ever more devious ways.Such a ransomware variant has already been discovered using an innovative system to increase infections: the software turns victims into attackers by offering a pyramid scheme-style discount.If the victim passes on a link to the malware and two or more people install this file and pay, the original victim has their files decrypted for free.

6.9. Cyber risk insurance will become more common

This type of insurance will increasingly become part of operational risk strategy however, the insurance industry needs to tailor products specific to client needs and not just provide blanket cover as extensions to existing risks. As the industry evolves we might see cyber insurance covering for loss of reputation and trust with their customers, loss of future revenue from negative media or other exposure, and improvement costs for security infrastructure or system upgrades.

6.10. New job titles appearing – CCO (Chief Cybercrime Officer)

In the aftermath of the TalkTalk data breach, MPs recommended appointing an officer with day-to-day responsibility for protecting computer systems from attack.

6.11. Will 2019 see organisations looking to appoint a chief cybercrime officer?

The CCO would be responsible for ensuring that an organisation is cyber-ready, would bear the responsibility for preventing breaches, would take the lead if a breach did occur and provide a robust connection between the board and the rest of the company.

VII. Cyber security prevention plan :

While there is no simple, singular solution to combat hack attacks and deter criminals, a layered prevention plan is crucial. There are five main steps that a company should take to prevent serious damage from a cyber attack. They are as follows. [7]

7.1. Assess your current cyber hygiene :

The UK Government backs an innovative scheme called Cyber Essentials which is designed to help all companies improve their cyber hygiene. It's an essential requirement for any business bidding on government contracts, but it's beneficial for any company, as it's believed to reduce the risk of an attack by up to 80%. It results in a certification which demonstrates a commitment to protecting business and stakeholder data from threats – crucial for building customer trust. The scheme covers all essential controls such as firewalls, malware prevention and up-to-date software.

7. 2. Good housekeeping :

There's no replacement for the basics. Updates and patching should be performed regularly — WannaCry, the ransomware that caused chaos across the world, exploited unpatched Windows systems to spread malware. Businesses should steer away from legacy systems like Windows XP, as these no longer receive updates and are especially vulnerable to attack. Get in the habit of conducting regular routine maintenance and audits, and seek a service provider if necessary, which can use specialist software to block ransomware strains.

7.3. Raise awareness, stay vigilant :

Awareness should always underpin your prevention plan. SMEs are often targeted as the way in for financial attacks through phishing or impersonation with the aim to extract financial data or currency. This is often due to it being easier to take advantage of human behaviour to target specific individuals who may not have had the right training. Whether it's lack of awareness or just lazy decisions, they need to be properly trained on the risks and repercussions, along with potential hacking tricks as the majority of malware still requires a human action to initiate it.

7.4. Layered prevention approach :

There are business-grade security solutions that can help protect the network and users from would be attacks such as anti-virus, anti-spam and business grade firewalls. Businesses should always invest in a layered defence strategy, as the more comprehensive the set up is, the less chance an attack will succeed as it has to pass through the various layers. Avoid free products and solutions which claim that they can keep malware off your PC. Windows Defender, for instance, doesn't stop adware or Potentially Unwanted Programs (PUP) and doesn't possess the accuracy and effectiveness that more sophisticated prevention tools do. Paid-for prevention tools are a small price to pay for the reassurance of digital safety. The cost of a hack to a business would be much more than the cost of the prevention technology.

7.5. Better safe than sorry :

While it's important to be proactive, businesses need a recovery plan in place in the event of a disaster or any downtime. A staggering 60% of businesses that encounter an attack go out of business in their first year, because of attacks to their network and users. While the big dogs like the NHS, Sony and Equifax dominate the headlines when they suffer attacks, it's the Small & Medium Enterprises (SMEs) that are secretly suffering the worst due to factors such as the human element and not prioritising investments, as mentioned above.

Under General Data Protection Regulation (GDPR) legislation, you must have a plan in place to be able to restore data, whether it's a cyber attack, file corruption or simple data loss, otherwise you risk non-compliance. IT continuity is the bread and butter of so many businesses, and you must make sure that you have a backup and business continuity plan to prepare, should the worst happen. Seek Disaster Recovery as a Service (DRaaS) to protect critical business data and get operational again after a disaster.

While there is not a simple, singular solution to combat hack attacks and deter criminals, a layered prevention plan is crucial. Follow these steps, and data misuse and abuse can be minimised, while still enabling your business to take advantage of the growing opportunities the internet can harness.

VIII. Cyber Insurance

Unfortunately, data breaches and other cyber crimes are becoming way too common. In the past couple of years, data breaches have resulted in major fines and legal fees – not to mention headaches – for a discount retail chain, one of the nation's largest banks, a well-known health insurer, an entertainment network and the government. But it's not just large organizations that are susceptible to being hacked or getting a virus. Nearly 55% of small businesses have experienced a data breach and that 53% have had multiple breaches?. A data breach can damage more than just your small-business computer system – it also can damage your reputation and put your customers and/or employees at risk. A bad actor deploys ransom ware into a manufacturing company's network environment which freezes up operations and delete files until it receives ransom payment. This could lead to direct revenue loss in a business interruption claim while operations are down and sales are halted. There could be consequential damages if this causes supply chain issues with its partners who are not receiving necessary component parts, thereby leading to third party claims. That's why cyber insurance can be a smart precaution for any size business.

8.1. What is cyber insurance?

Cyber insurance generally covers your business' liability for a data breach involving sensitive customer information, such as Social Security numbers, credit card numbers, account numbers, health records etc., General liability insurance covers bodily injuries and property damage resulting from your products, services or operations. Cyber insurance is often excluded from a general liability policy.

8.2. Cyber insurance coverage :

The cyber insurance covers the following.

- Legal fee and expenses
- Notifying customers about a data breach
- Restoring personal identities of affected customers
- Recovering compromised data
- Repairing damaged computer systems

IX. CONCLUSION

Throughout the year 2018, many cyber breaches were reported. With a different issue almost every week throughout the year, cyber security is at the top of bysiness owners' minds. Also, this is not something that experts foresee ending any time soon. As such there are some of the things you shall have to pay attention in the year 2019.Latrobe University claims that it takes a combination of education and awareness to prevent cyber attacks from occurring. Standard defense practices are only as strong as their weakest link, which is why it's so important to train your employees regarding phishing and spam emails. These act as an entryway for malware, so one should:

- Use reliable, well-known security and antivirus software
- Make sure devices update automatically
- Don't click on email attachments from an unknown source
- Don't add people to your social media network unless you know them
- Don't use apps or software from free sites – Buy them from the official website instead
- Routinely change passwords, making sure they contain a unique combination of numbers and letters (in both upper and lower case)
- Don't use old, unsupported browsers

With these practices in place, we can expect a higher level of cyber security in the year 2019.

X. REFERENCES

[1]. Gemalto, International data security company
[2]. Michael Fitzgibbon, Slice Insurance Technologies
[3]. Dr. Andrew Shields, Cambridge Research Laboratory of Toshiba Research Europe,
[4]. Scott Carter, Senior Manager – US, Venafi
[5]. Jan Oetjen, CEO of GMX
[6]. Andy Taylor, lead assessor, APMG International
[7]. James Healey, Managing Director, Air IT

Cite this article as :

Y. V. Sai Bharadwaj, Sai Bhageerath Y.V, Prof. Y.V.S.S.S.V. Prasada Rao, "Cyber Security, Challenges, Some Practical Solutions", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 1, pp. 79-87, January-February 2019.
Available at doi :
https://doi.org/10.32628/CSEIT19519
Journal URL : http://ijsrcseit.com/CSEIT19519