2017

CYBER ATTACK TRENDS

WHITEPAPER

CYRAATEK

CONTENT

Executive summary 3

Understanding the threats of cyber attacks on SMEs 4

Emerging threats and challenges - Internet of Things 5

Analysis roundup 9

Notable cyber attacks in 2016 10

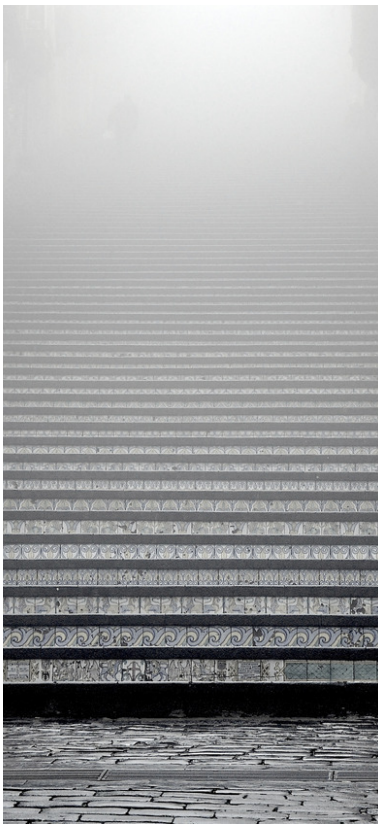
Real value of penetration testing 10

A closer look at the advantages of periodic penetration testing 11

Cyraatek's cyber threat predictions 12

Brief overview of services – Cyraatek 13

Executive Summary



In this whitepaper, Cyraatek have reviewed Cyber security issues affecting many areas of digital technology. From IoT devices (Internet of Things) and smart automobiles to commonly used computers and typical corporate servers, we have focused our analysis on current attack trends and the effects of intrusion on corporations. The aim of this publication is to build awareness among our readers about attack and defense trends currently occurring in the digital market.

This report has been complied after close collaboration between multiple departments and also includes comprehensive insight from our team of professional security researchers. External resources such as recent research paper on the topic, books, articles and guidance from academics involved in the area of security research, has also been sought during the production of this document.

By gathering information from sources mentioned above, we have created a guide, which will aid the reader of this report in understanding the current threat landscape in the security industry. Additionally, this report also provides an insight into Cyraatek solution's background and how we aim to revolutionize the security industry by offering affordable and efficient security solutions to our clients.

Understanding the threats of cyber attacks on SMEs.

There is an immense shortage of skilled security workers, which is preventing businesses from bolstering their networks against attacks.

Computers have revolutionized our lives since the day they came into existence. From putting a man in space, to performing automated complex medical surgeries, digital technology is assisting us in every aspect of our lives. Therefore, it is undebatable that computers are now an integral part of human life. However, this necessity of life has also attracted a lot of interest from malicious attackers, informally referred to as hackers, who perform many attacks in this illegal trade to bring harm to the ordinary users, or financial gain to themselves. Many enterprises fall victim to these attacks and face substantial financial losses, data breaches and subsequent lawsuits, resulting in further financial implications. For example, a report released by McAfee in 2014 titled – 'Net Losses: Estimating the Global cost of Cybercrime' predicted that the annual estimated losses to Global economy due to cybercrimes could be as high as $575 billion in 2015. Further analysis conducted by a firm 'Cyber Security Ventures' in 2016 concluded that the total global cost of cyber crimes would reach around $3 trillion by 2015 and could be as high as $6 trillion by 2021.

Digital attacks against Small and Medium sized Enterprises (SMEs) are so frequent that they are now considered a common occurrence worldwide. Primarily due to the fact that small enterprises under appreciate the threat of cyber security, and secondly have limited funds to implement security efficiently. There is also an immense shortage of skilled security workers, which is preventing businesses from bolstering their network against attacks. In addition, soaring cost of security auditing solutions and security awareness training for employees, is also one of the reason why some SMEs have not deployed effective digital defences against attackers. Cyraatek has identified this serious gap in the market, and in collaboration with Innovate UK, is offering affordable security solutions to SMEs

According to Gov.uk, recent research undertaken by the UK Government revealed that nearly two thirds of large businesses suffered an attack or an IT related breach on their equipment in 2015. The same article refers to the UK Government's strategy to combat cyber attacks by dedicating £1.9 billion in investment, to bolster IT infrastructure as well as funding a new 'National Cyber Security Centre', which was inaugurated by the Queen in February 2017.

However, despite all the measures being taken at a higher level, the threat of digital attacks against businesses is likely to intensify. It would not be an understatement to say that the threat of cyber attacks is at an all time high, and analysis of trends indicates that it will continue to rise.

We are observing an increased risk of cyber attacks against technology users of all types and business of all sizes. The attacks are getting more sophisticated in nature. Consequently, it is becoming harder for businesses to stay on top of this threat, as some attackers have devised complex techniques to stay unnoticed and unidentified.

Allianz Insurance, one of the top players in the UK insurance industry, annually issues a report on the threats faced by modern world. Their 2016 report claims that the cyber related incidents have increased by over 17% compared to 2015, making it one of the biggest threats businesses are facing today.

The exponential growth of cloud and mobile technologies as well as the Internet of Things (IoT) is making considerable impact on the population. Not only enterprises now have a diverse playing field to develop and evolve newer business models, but at the same wide spread adaptation of IoT is also redefining substantial expansion in the current product offering and branding strategies. However, continued evolution of these services has also brought unanticipated challenges for the users of these technologies. Fundamentally, lack of awareness about rapidly evolving security issues is the reason most users and companies are failing to protect themselves from cyber attacks.

Rapid expansion of IoT devices coupled with inadequate security mechanisms employed by these devices, will lead to substantially greater cyber security risks in the near future. the consequences of exploitation on such a borad level will have drastic effects, not just n businesses but the overall technology users, from individual to Governments. The lack of awareness with regards to IoT security, among its users, is worrying to say the least.

Lack of awareness about rapidly evolving security issues is the reason most users and companies are failing to protect themselves from cyber attacks.

Emerging threats and challenges - Internet of Things

Simply put, IoT is the inter-networking of physical devices, comprising of smart everyday objects and connected devices (i.e. fridge, toasters, lights), with network connectivity that enables these objects to collect and exchange data seamlessly. In effect, IoT is a pervasive technology, which spans across various sectors.

Today, it is not uncommon to see food storage shelves in homes that can keep track of the items being consumed and then re-orders the food accordingly, without any requirement for human interaction.

Similarly, we now have products in the market like smart kettles, that can be activated remotely with a touch of a button on a mobile phone, or location aware thermostats, that can turn the heating on when they detect you are leaving office for home and always-on voice activated virtual assistants, with the ability to carry out precise data analysis to support us in our daily life functions.

Recent introduction of Amazon Dash button for example, brings convenience and ease in the lives of many of their customers. Rather than looking for a phone, tablet or a computer to order items, Amazon customers can simply press the wirelessly connected standalone button, which then sends a ‘purchase’ command to amazon, so delivery of the pre-specified goods (i.e. toilet papers) can be arranged.

We as humans are completely surrounded now by IoT devices. In smart cities, for example, IoT devices are used to manage smart parking, traffic congestions, and lighting and to study changing habits of urban population. Smart sensors are being used to measure temperature inside industrial and medical storage facilities with sensitive merchandise. IoT devices with auto diagnosis capabilities are being used in vehicles to send real time alarms to emergency services, in case of an incident. From waste to premium food products, waste in waste management facilities is being monitored and sorted by IoT objects. Additionally, IoT devices are now even being used to enhance wine quality, by monitoring parameters including soil moisture and trunk diameter in vineyards.

The reality is that the IoT industry is expanding rapidly. According to Gartner Inc., there will be 21 billion connected IoT devices by the end of 2020. Another esteemed news source ‘Forbes’ reports that the number

Sudden growth and adoption of IoT in the past couple of years has given rise to new attack vectors.

the IoT devices will reach 75.4 billion by 2025.

Analysis of the reports relating to this industry shows that the exponential growth in the IoT device uptake has taken academics, scientists and technology sector in general, by surprise. The large-scale adoption of IoT is having a similar effect on the IT industry and consumers as the IPhone had, when it was first launched in summer 2007. However, in the case of IoT, no one anticipated that this industry could become so huge relatively overnight. Although, it can be argued that devices connected to wireless Internet has now been in existence for well over two decades, it is only in the last three to four years that we have observed a huge rise in their uptake, particularly in within the consumer market, transforming everyday objects into smart devices. However, sudden growth and adoption of IoT in the past couple of years has given rise to new attack vectors.

A point to note here is that the problem with IoT sector is not its rapid growth, but the lack of security within devices, and in the way they connect to the Internet. After thorough analysis of varying types of IoT devices, there is a mutual consensus between academics, researcher and ethical hackers that objects bearing IoT hallmarks have generally much weaker security compared to computing devices we traditionally use.

The most recent result of such security lapse is the outage of some of the top Internet websites that occurred in October 2016. Experts describe this outage to be one of the largest and most organized attacks of its kind in the Internet history. To facilitate the offensive, attackers hacked a large collection of IoT devices using a malware, now known as ‘Mirai’, which utilised brute force and dictionary attack methods to break into poorly secured IoT devices. Once in control, the malware further infected the devices with malicious code so they could be turned into bots, which could then perform a variety of automated tasks on behalf of their masters.

A large collection of botnets is all the hackers needed to launch their attack. The botnets were used to direct massive amounts of bogus Internet traffic (approximately 990Gbps) towards the infrastructure of Dyn, an Internet performance management company and a cloud service provider, allowing the hackers to send their servers off-line for considerable amount of time. Consequently, companies who relied on Dyn for their services, also went off-line for the duration of the attack. Some of the well-known companies that became victims of this attack included Reddit, Paypal, Twitter and Spotify, among many others.

The danger of IoT hacking is real and can be life threatening in some cases. For instance, imagine hackers taking control of the devices embedded into humans, to assist them with their bio-functions. Once a session is established between a hacker and medical IoT device, hackers can relatively easily disturb digital mechanics of the device and intentionally or unintentionally cause damage or even death to the wearer. For example, the Food and Drug Administration (USA) released a statement in February 2017, in which they warned that some pacemakers are vulnerable to hacking. The advisory stated that under certain conditions, attackers could take complete control of the pacemaker, send modified commands to the device, in order to achieve complete battery depletion and even administer inappropriate pacing or shocks to the wearer.

There have also been reports in the media relating to successful unauthorized takeover, by security researchers and malicious attackers, of autonomous and semi-autonomous automobiles and even airplanes, in the recent months. Autonomous cars rely heavily on wireless networks and satellites to perform their functions. By using unsecured and weak rely heavily methods of communications, manufacturers of autonomous cars

on wireless networks and satellites to perform their functions. By using unsecured and weak methods of communications, manufacturers of autonomous cars could be inadvertently putting the users in danger.

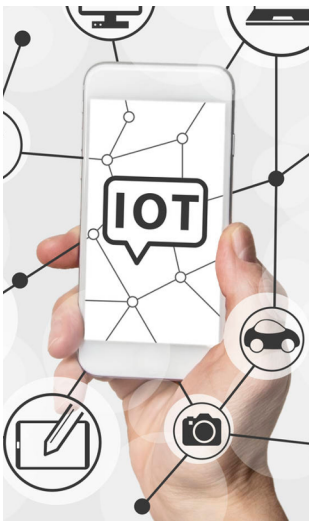
Wired, a reputable news source among technology enthusiasts, reports about a hack conducted by two security researchers on Chrysler's Jeep Cherokee in 2016. The article states:

"By sending carefully crafted messages on the vehicle's internal network know as a CAN Bus, they're (security researchers) now able to pull of even more dangerous, unprecedented tricks like causing unintended acceleration and slamming on the car's brakes or turning the vehicle's steering wheel at any speed."

By utilizing zero day exploits, which are security flaws that are not previously known, hackers are now successfully chartering this preciously invulnerable territory of drone and smart car attacks. We anticipate these type of attacks will become an even bigger problem for manufacturers, users and Governments, compared to attacks on small immobile devices.

In March 2016, the Federal Bureau of Investigation released a public announcement (I-031716-PSA) in which it warned that modern motor vehicles are increasingly susceptible to remote exploits and urged the consumers to be cautious and recommended measures to minimize the possibility of an attack.

Increasing interest from hackers in IoT devices suggests that the October 2016 attack mentioned above is just the beginning. A hacked IoT system can also potentially be used as a gateway to any other connected devices, for example smart mobile phones, or enterprise infrastructure. Once attackrs are inside an IoT system, they do hace the ability to transmit malicious code through the IoT communication system to connected devices or systems. Unless device developers and manufacturers provide this issue the attention it deserves, we anticipate IoT hacking will become more mainstream route of attack among hackers.



Moving forward, consumers of IoT products also have a responsibility to play their part in securing their devices. When it comes to smart devices, it is clear that some manufacturers are slow in issuing software updates. However, if a devices is already exploited by an attacker, it is probable that the attacker will set the device to refuse any manufacturer updates to allow them to continue with maximum control over the device. In this scenario, it is the responsibility of the device's user to check that their devices are up to date with manufacturer updates and that they are not being manipulated, for example being uses as a botnet or as surveillance device. For instance, Virtual Assistants like Amazon's Echo and Google Home are increasingly becoming part of a normal household. These assistants contain an always-on microphone, and they have the potential to act as an excellent spying device. In addition, customer data and search history are stored on these devices. This data can easily be obtained by attackers, providing them with useful information about the habits and routines of a household.

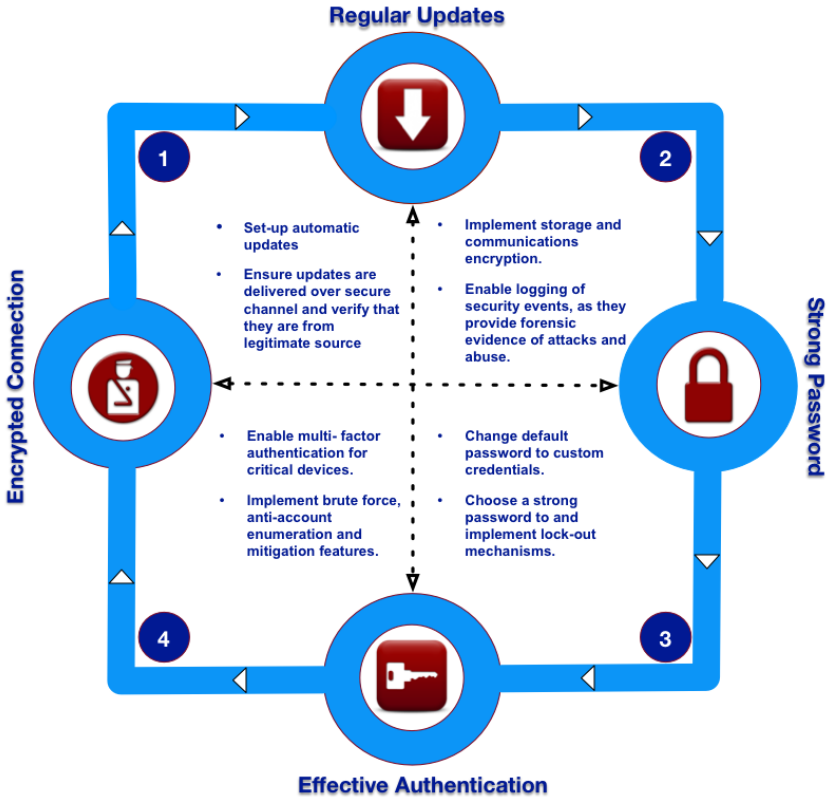
In March 2017, Wikileaks claimed in leaked intelligence documents that the CIA is running a secret computer hacking program, providing its agents with tools to hack and listen into everyday devices such as TVs, phones and tablets. The report also mentions that CIA has acquired the capability to target cars, which are operated by onboard computers with Internet connectivity. Wikileaks further claimed that once in control of the vehicles, CIA could stage a crash, resulting in an assassination but making the crash appear to be an accident.

'THERE HAVE BEEN REPORTS IN THE MEDIA RELATING TO SUCCESSFUL UNAUTHORIZED TAKEOVER, BY SECURITY RESEARCHERS AND MALICIOUS ATTACKERS, OF AUTONOMOUS AND SEMI-AUTONOMOUS AUTOMOBILES AND EVEN AEROPLANES, IN THE RECENT MONTHS. '

Following this revelation, Wikileaks began dumping these CIA hacking tools on the Internet, in the hope that manufacturers will study these exploits and take measures to ensure that these vulnerabilities are patched. However, these hacking tools have now ended up in public domain and are being accessed by malicious hackers, who have now garnered even stronger capability to attack everyday smart devices. In order to protect themselves, enterprises need to adhere to security standards as a minimum. Therefore, the most efficient way to ensure that your smart devices are safe and secure is by considering the four steps below:

1. Making sure that Internet connected devices, connected networks and operating software are running the most up to date patch issued by the manufacturer.
2. Ensuring that all communications and data transfer over the network is encrypted. This allows the user to create a barrier between yourself and an attacker
3. It is also strongly recommended that a strong password be used wherever possible. Readily available hacking tools can easily crack weak passwords. A strong password is usually defined as having a minimum length of at least twelve characters, comprising of unique mixture of letters, numbers and symbols, you can reduce the probability of your device getting hacked by an attacker
4. Use multi-factor authentication for critical devices and infrastructure to stop unauthorized access. Dual layer authentication is also an excellent mitigation mechanism to repel brute force attacks.

Periodic penetration testing exercises from an accredited security auditing company is also recommended, as these tests can substantially enhance chances of discovery of any potential anomalies or holes in the security of smart devices or the systems they are connected to. By simulating a real-world attack scenario, a penetration test can determine the vulnerabilities that exist in your systems, enabling you to understand and improve your ability to deal with the attack, when it occurs



Analysis roundup

Dell is one of the most recognizable name in the IT industry, serving corporations and end users of all types. The annual cyber security threat report published by Dell in 2016 shows a worrying but unsurprising surge in the cyber crimes being committed across the globe. Their report demonstrates the severity and magnitude of the ever-increasing attacks on big names, such as Amazon, Bank of Scotland, Ashley Madison, Harvard University and many more.

Overall, the report by Dell presented an alarming rate with which viruses, Trojans and increasingly sophisticated exploit kits are being used to target computing and IoT devices. However, critical servers currently remain the primary target of the attackers in the category of intrusion attacks.

Another company, FireEye, which focuses exclusively on the cyber security, published their report in early 2017 on the emerging trends in attack methodology employed by malicious attackers and digital defense strategies. Commenting on the rise of sophisticated attack methods, the editor of the report states:

"Financial attackers have improved their tactics, techniques and procedures (TTPs) to the point where they have become difficult to detect and challenging to investigate and re-mediate".

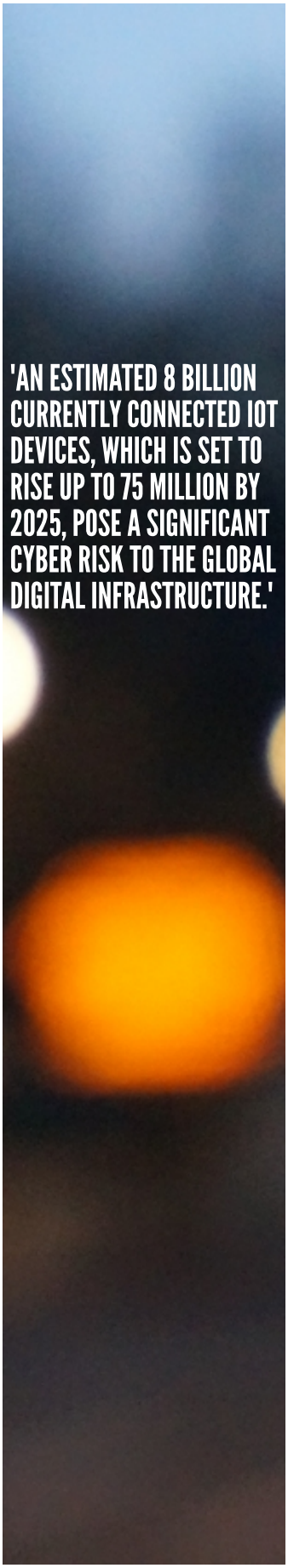
Research conducted by FireEye highlights how scammers are changing their tactics to bypass complex authentication protocols. For instance, attackers are increasingly developing malicious applications that can overcome two-factor authentication requirements by embedding malicious applications with Open Authentication (OAuth) tokens. OAuth is an open-source standard and is widely used by developers to obtain authority to share information without the need for a password. As soon as a victim mistakenly authorizes the malicious application's request for access, the attacker acquires the ability to gain entry to all data held on victim's account, for example their Google account, and can retain permission to access the account, even when the password is updated or changed.

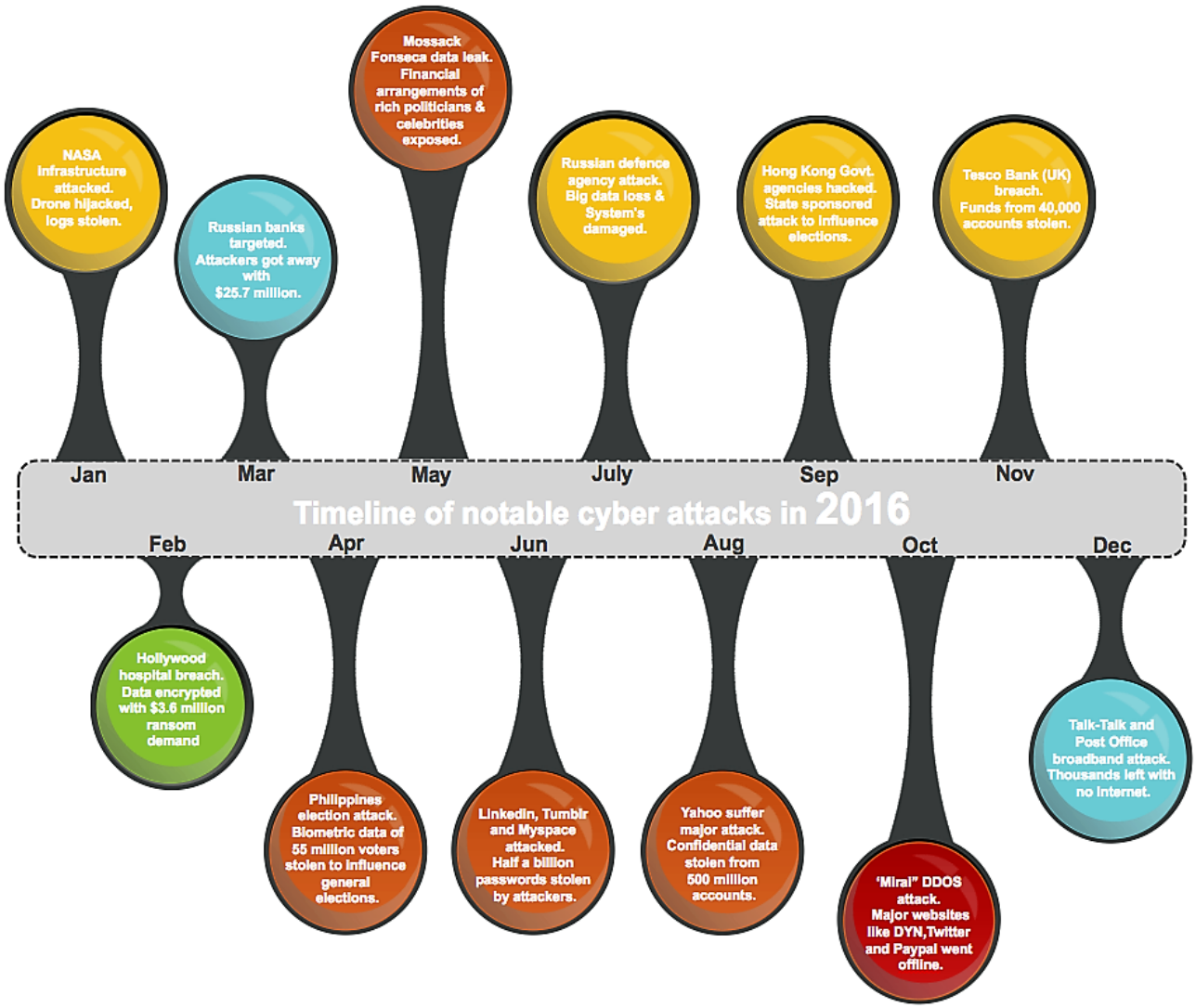
Infosecurity, Europe's largest Security event organizer, stated in their magazine:

"Hackers spend 200+ days inside [an IT] system before discovery."

By any measure, two hundred days is a considerable amount of time for anyone to monitor servers, to extract and analyse data. However, the same article also states that the discovery of a breach after intrusion occurred used to be around 243 days in 2012. Hence, we are making progress when it comes to attacks being detected and remedied. This improvement can be associated with a small increase in the level of awareness of security threats. In addition some enterprises, particularly larger enterprises are now using security auditing services, which are now being offered and promoted more, compared to the past.

The growth of IoT and mobile devices, with the capability of exchanging data over the Internet, has created the biggest digital attack vector known to the technology industry in recent history. While it is probable that with education and persistent reminders, IoT developers will start taking security more seriously, evidence suggests that it has not happened yet. Which is why an estimated 8 billion currently connected IoT devices, which is set to rise up to 75 billion by 2025, pose a significant cyber risk to the global digital infrastructure. Current attack trends should lead companies to re-think their defense strategies in the face of repeated cyber threats. As a minimum, SMEs should adhere to security protocols and offer security training to its staff. In addition SMEs should consider committing to regular security auditing and penetration testing exercises, as well as improving staff awareness on security issues, to prevent them from becoming a victim of social engineering attacks. The next section of this white paper has shed some light on the benefits of regular penetration testing.





Notable Cyber Attacks in 2016

Real value of penetration testing

In today's convoluted security landscape, it can be hard for businesses to keep track of all the emerging threats. As more and more zero day exploits are exposed by the researchers, it is more important than ever to have an understanding of what problems a business might suffer, if they face an attack on their infrastructure.

During an attack, companies may suffer loss of their services. In the aftermath of the attack, as well as suffering loss of reputation, companies can also receive fines from regulatory authorities for failing to take sufficient steps to protect their systems, losing customer data, as well as the possibility of lawsuits from their customers. So, to protect oneself from the possibility of an attack, penetration testing is an exercise, which is undertaken by security professionals to determine and assess vulnerabilities in a system.

Penetration testing is essentially a practice of testing computer systems against known technical weaknesses, to determine the type of vulnerabilities residing in the software, hardware or web applications. The main purpose is to find vulnerabilities and make it difficult for malicious attackers to gain access to your infrastructure and data. After completion of the testing, the penetration tester prepares a detailed report with a list of all vulnerabilities identified during the test and a set of recommendations. This report enables the host company to fix or patch any technical or procedural weakness in their infrastructure.

A closer look at the advantages of periodic penetration testing

It is reported by Navigant, who operate as a specialised expert service firm, that the average cost of security breach in 2013 was £4,976,900. Navigant also reported that security testing performed by 'Cenzic Security' in the same year, led to discovery of technical flaws in 96% of the cases. An average loss of £4,976,900 is a substantial amount, in contrast, security testing would only cost a fraction of this amount. These incredible statistics demonstrate a strong case for why corporations must integrate regular penetration testing into their security procedures.

It is recommended that a security evaluation is requested periodically, especially during the creation of a new infrastructure or during every significant alteration to an organisation's IT infrastructure. If the evaluation cannot be carried out during an alteration phase, it should be carried out after its completion to highlight new vulnerabilities. A detailed penetration test provides the following benefits to the client:

1. Testing of defense capability

One of the primary reason corporations get their infrastructure rested is to determine vulnerabilities on their systems. A penetration test not only reveals the flaws, that can be exploited by the attacks, but the assessment can also help the organization understand their readiness to deal with a breach, should an attack occur.

2. Helps achieve certifications and compliance with geographical, industry or legal regulations

There is often a legal requirement for corporations and businesses to perform penetrations tests against their information systems, before they can apply for certifications, such as ISO27001. Therefore, security testing should be carried out to facilitate this compliance. The Security testing can include testing for this specified certifications, if required.

3. Protection of data, clients and reputation

According to research, most corporations consider cyber security to be a concern. Instead, they consider the main threat to their reputation to be business continuity. In essence, a security breach can directly affect business operations and logistics. When businesses consider the cost of penetration testing, this should be compared against the cost of the loss of service or business continuity, potential loss of data, damage to reputation and subsequent lawsuits and fines that would result if a breach occurs.

4. Market Competition

To be competitive in the market, SMEs often have to demonstrate to their customers that they have taken sufficient security precautions to ensure protection of data and have established disaster recovery plans. A certificate of completion in security auditing and penetration test can help assure customers that a responsible company is looking after their affairs.

5. Risk Assessment

Another benefit of periodic penetration testing is to satisfy the risk assessment and planning elements in a business. It is important for SMEs to have a risk based thinking with good understanding of information security and why it is crucial for business operations. Penetration testing can help businesses understand the weaknesses in their technical infrastructure and the report, which is provided, comprises of an extensive list of recommendations that enterprises can implement to harden their system against malicious attackers. This list of recommendations will be graded to differentiate the effect that each recommendation will have on the system.

In short, not only do corporations need to take the four steps listed above to strengthen their systems, they need to go above and beyond normal business practices to stay on top of security threats which are continually evolving. The security challenges in today's digital world are dynamic, daunting and convoluted. Therefore, robust cyber security, continual testing of infrastructure and regular training regarding the security outlook of employees should be the top priority of all businesses that have an IT infrastructure, not just those who are security conscious. A holistic and comprehensive strategy that deals with risk management, cyber security and continuous penetrations testing, will help the businesses in protecting themselves from the dangers of cyber attacks.

Cyraatek's cyber threat predictions

This section offers short to long-term insight for companies looking to stay ahead in the race against attackers. The content below predicts key development and forecast trends that are likely to occur over the next few years.

• Ransomware: The availability of various user friendly ransomware deployment kits has enabled even the low-tech criminals to enter sphere of cyber crime. This is likely to cause further increase in Ransomware attacks on technology users of all types.

• Increase in Data Breaches: With recent attacks on LinkedIn, Target, Wonga, NSA, Cloudflare, CloudPets and many more, attackers are actively targeting institutions for information. We anticipate that in the coming years, this trend is likely to continue with many more organised cyber assaults on consumer data companies.

• Phishing attack: SaaS cloud model is susceptible to phishing and server cracking attacks. Over the years, we have seen advances in complexity of phishing attacks. Criminals now have the ability to forge SSL certificates, which renders built it browser protection against phishing useless. Because of the ease with which certificates can now be forged, we predict substantially more attacks, as more businesses move their data to cloud.

• Increase in state-sponsored attacks: In the light of Stuxnet, The Shadow Brokers leaks, North Korea hacks, we will continue to witness increase in reported state-sponsored attacks as Government's desire to know more about what their enemies and allies are doing.

• Smart Grid Attacks and IoT: In the recent years, there been a significant rise in the adoption of smart grid and IoT devices. Many cities are now competing with each other to implement smart features in their infrastructure. However, this technology suffers from serious vulnerabilities. As the uptake of this technology increase, attackers will have even greater availability of vulnerable of appliances, which they will potentially hack for malicious purposes.

To protect oneself from ever increasing threats of cyber attacks, enterprises and users of technology needs to be ready with concrete defence strategies, as the cyber threat landscape is continually evolving in complexity.

By efficiently utilizing technical and human resources to protect the network and connected devices, companies will not only protect themselves from harm and potential financial loss, but also play their part in making cyberspace more secure and safe online users. In short, the more enterprises learn about threat prevention, detection and response, the faster they will become at preventing and mitigating cyber attacks.

Brief overview of services - Cyraatek

In today's growing digital world, protecting your company's applications, information and infrastructure is becoming increasingly challenging. Cyber criminals are becoming more innovative with new attacks, and technologies such as IoT, Cloud, Visualization and Collaboration tools create more vulnerabilities, that can expose your business to more attacks.

'WE OFFER OUR CLIENTS END-TO-END SECURITY SOLUTIONS FROM AUDITING TO PENETRATION TESTING, SECURITY SOFTWARE AND HARDWARE SOLUTIONS TO TRAINING ON SECURITY

Cyraatek has responded to these security challenges by providing affordable and dynamic services that extend beyond just technology. An arm of RAA Technology Solutions Ltd, Cyraatek is a fast growing technology solutions providers, with clients in over 10 counties globally. With a healthy list of clients in Europe and as well as Africa, Cyraatek has gained enormous reputation in the security industry, while also helping its clients implement, innovate and improve business performance.

In partnership with sister company RaaIT (raait.co.uk), we provide wide range of services from planning, supplying and installation of IT infrastructure to upgrades and repairs. In addition, Cyraatek is also a provider of bespoke security solutions and cyber awareness training, to protect organisations from cyber threats. We include people, culture, processes and the physical environment to make your business as impenetrable as possible against the threats from Cyber criminals. By offering bespoke cyber security solutions to resolve challenges across a wide spectrum of sectors, Cyraatek has become the ideal IT security provider of many SMEs. Cyraatek is also being supported by Innovate UK initiative.

Credits

Akin Ande
(Chief Executive Officer)

Akin is the founder and leader of Cyraatek. In the past Akin has been involved in multiple successful Tech companies. However, his attention is focused on growing Cyraatek into a global player. With the vision for providing high quality and affordable service, Akin is on track to make Cyraatek a well-known and reputable brand in the IT security industry.

Akin is a Software Engineer, graduating from Manchester University in 2008, as well a family man and a father of two children. He has a passion for entrepreneurial projects and raising money for noble causes.

Jibran Saleem
(Cyber Security Consultant)

Jibran was appointed as a Cyber Security Developer in March 2017, after completing his MSc in Computer & Network Security with a distinction.

Jibran previously held the position of System's Administrator at HSBC and won numerous awards for his services. Jibran is a keen technology enthusiast with interest in penetration testing, IoT and network defenses.

Daniel Adebayo
(Senior Security Consultant)

Daniel is a senior security consultant at Cyraatek with a passion for information security. He has keen interest in IoT security. Previously a network engineer, Daniel has dedicated his career to designing and securing information systems.

Daniel earned his B.Sc at Covenant University, amongst other certifications he holds a CCIE, CEH, PCNSE, CCSA and currently working towards obtaining OSCP certification.

Contributing Experts

Ruth Irwin
(IoT Specialist)
Cyraatek Ltd.

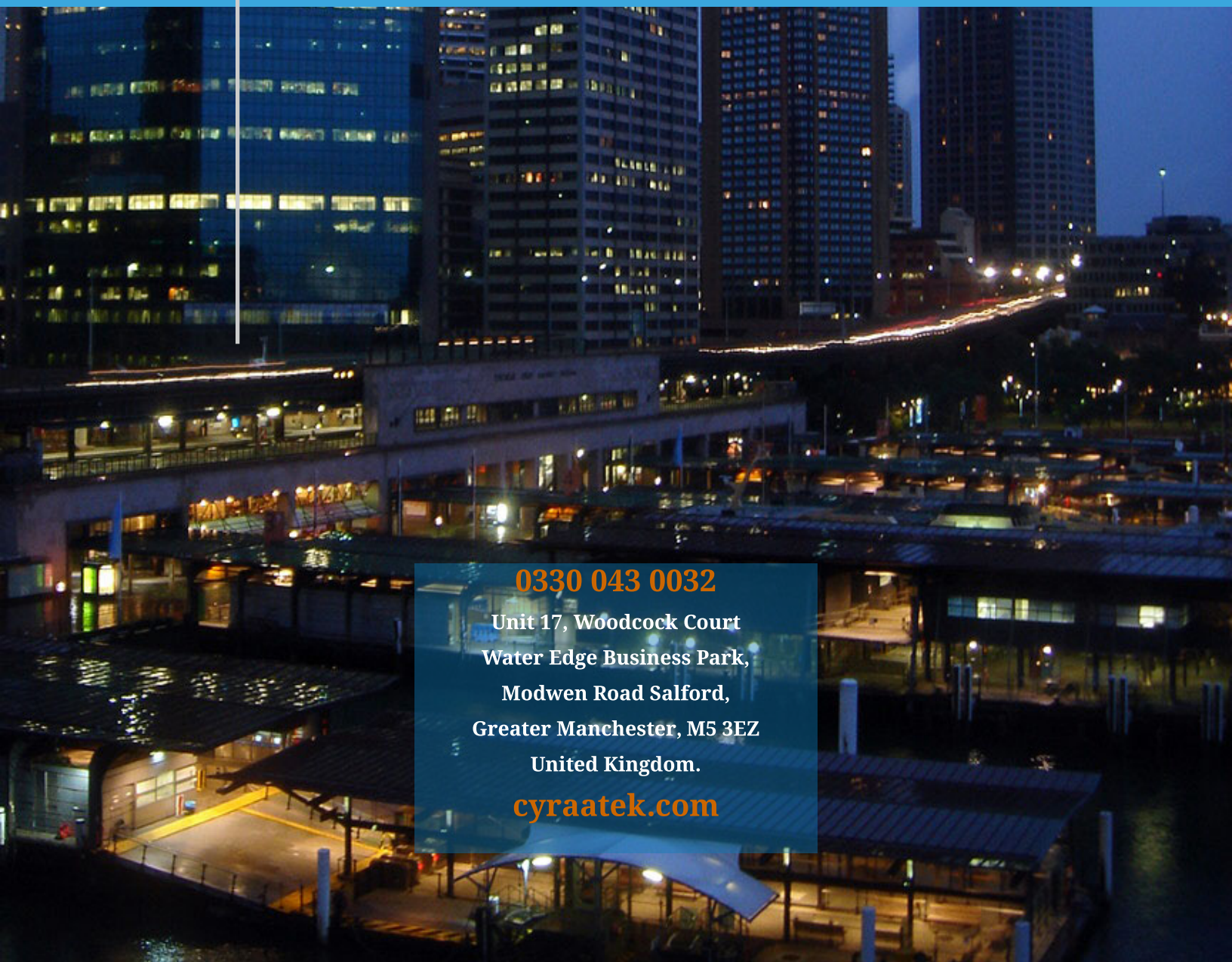
Dr. Mohammad Hammoudeh
(Senior Lecturer)
Manchester Metropolitan University

We would also like to thank **Toyinsola Oduyale** for assisting us in the design and development of this whitepaper.

2017

CYRAATEK

www.cyraatek.com



0330 043 0032

Unit 17, Woodcock Court
Water Edge Business Park,
Modwen Road Salford,
Greater Manchester, M5 3EZ
United Kingdom.

cyraatek.com