CHAPTER 1

1. INTRODUCTION

1.1 Introduction

Data security is crucial for all small businesses. Customer and client information, payment information, personal files, bank account details - all of this information is often impossible replace if lost and dangerous in the hands of criminals. Data lost due to disasters such as a flood or fire is devastating, but losing it to hackers or a malware infection can have far greater consequences. How you handle and protect your data is central to the security of your business and the privacy expectations of customers, employees and partners.

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

Information security protects the integrity and privacy of data, both in storage and in transit.

Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

1.2 The scale of the cyber threat

The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by Risk Based Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.

Medical services, retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.

With the scale of the cyber threat set to continue to rise, the International Data Corporation predicts that worldwide spending on cyber-security solutions will reach a massive $133.7 billion by 2022. Governments across the globe have responded to the rising cyber threat with guidance to help organizations implement effective cyber-security practices.

In the U.S., the National Institute of Standards and Technology (NIST) has created a cyber-security framework. To combat the proliferation of malicious code and aid in early detection, the framework recommends continuous, real-time monitoring of all electronic resources.

The importance of system monitoring is echoed in the “10 steps to cyber security”, guidance provided by the U.K. government’s National Cyber Security Centre. In Australia, The Australian Cyber Security Centre(ACSC) regularly publishes guidance on how organizations can counter the latest cyber-security threats.

CHAPTER 2

2. TYPES OF CYBER THREATS

2.1 Types of cyber threats

The threats countered by cyber-security are three-fold:

1. Cybercrime includes single actors or groups targeting systems for financial gain or to cause disruption.

2. Cyber-attack often involves politically motivated information gathering.

3. Cyberterrorism is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

- Malware
  Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

  There are a number of different types of malware, including:

- Virus:
  A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

- Trojans:

  A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

- Spyware:

  A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

- Ransomware:

  Malware which locks down a user’s files and data, with the threat of erasing it unless a ransom is paid.

- Adware:

  Advertising software which can be used to spread malware.

- Botnets:

  Networks of malware infected computers which cybercriminals use to perform tasks online without the user’s permission.

SQL injection

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim’s device and the network.

Denial-of-service attack

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Latest cyber threats

What are the latest cyber threats that individuals and organizations need to guard against? Here are some of the most recent cyber threats that the U.K., U.S., and Australian governments have reported on.

Dridex malware

In December 2019, the U.S. Department of Justice (DoJ) charged the leader of an organized cyber-criminal group for their part in a global Dridex malware attack. This malicious campaign affected the public, government, infrastructure and business worldwide.

Dridex is a financial trojan with a range of capabilities. Affecting victims since 2014, it infects computers though phishing emails or existing malware. Capable of stealing passwords, banking details and personal data which can be used in fraudulent transactions, it has caused massive financial losses amounting to hundreds of millions.

In response to the Dridex attacks, the U.K.'s National Cyber Security Centre advises the public to "ensure devices are patched, anti-virus is turned on and up to date and files are backed up".

Romance scams

In February 2020, the FBI warned U.S. citizens to be aware of confidence fraud that cybercriminals commit using dating sites, chat rooms and apps. Perpetrators take advantage of people seeking new partners, duping victims into giving away personal data.

The FBI reports that romance cyber threats affected 114 victims in New Mexico in 2019, with financial losses amounting to $1.6 million.

Emotet malware

In late 2019, The Australian Cyber Security Centre warned national organizations about a widespread global cyber threat from Emotet malware.

Emotet is a sophisticated trojan that can steal data and also load other malware. Emotet thrives on unsophisticated password: a reminder of the importance of creating a secure password to guard against cyber threats.

End-user protection

End-user protection or endpoint security is a crucial aspect of cyber security. After all, it is often an individual (the end-user) who accidentally uploads malware or another form of cyber threat to their desktop, laptop or mobile device.

So, how do cyber-security measures protect end users and systems? First, cyber-security relies on cryptographic protocols to encrypt emails, files, and other critical data. This not only protects information in transit, but also guards against loss or theft.

In addition, end-user security software scans computers for pieces of malicious code, quarantines this code, and then removes it from the machine. Security programs can even detect and remove malicious code hidden in Master Boot Record (MBR) and are designed to encrypt or wipe data from computer’s hard drive.

Electronic security protocols also focus on real-time malware detection. Many use heuristic and behavioral analysis to monitor the behavior of a program and its code to defend against viruses or Trojans that change their shape with each execution (polymorphic and metamorphic malware). Security programs can confine potentially malicious programs to a virtual bubble separate from a user's network to analyze their behavior and learn how to better detect new infections.

Security programs continue to evolve new defenses as cyber-security professionals identify new threats and new ways to combat them. To make the most of end-user security software, employees need to be educated about how to use it. Crucially, keeping it running and updating it frequently ensures that it can protect users against the latest cyber threats.

CHAPTER 3

3. CYBER SECURITY TOOLS

3.1 CYBER SECURITY TOOLS

There are various tools are the modes of attack. And the malware are used for the totality of these tools. Examples are viruses and worms. Computer programs that reproduce the functional copies of themselves with varying effects ranging from emphasize and inconvenience to compromise of the confidentiality or integrity of information, and Trojan horses, destructive programs that pretence as benign applications but set up a back door so that the hacker can return later and enter the system. Often system intrusion is the main goal of system intrusion is more advanced attacks. If the intruder gains full system control, or „root" access, he has unrestricted access to the inner workings of the system .Due to the characteristics of digitally stored information the person with criminal intent will delay, disrupt, corrupt, exploit, destroy, steal, and modify information. The value of the information or the importance of the application will be depended, which the information are required and that such actions will have different effect with varying degrees of gravity.

1) Netsparker

Netsparker is an easy to use web application security scanner that can automatically find SQL Injection, XSS and other vulnerabilities in your web applications and web services. It is available as on-premises and SAAS solution.

Features

Dead accurate vulnerability detection with the unique Proof-Based Scanning Technology.

Minimal configuration required. Scanner automatically detects URL rewrite rules, custom 404 error pages.

REST API for seamless integration with the SDLC, bug tracking systems etc.

Fully scalable solution. Scan 1,000 web applications in just 24 hours.

2) Acunetix

Acunetix is a fully automated ethical hacking solution that mimics a hacker to keep one step ahead of malicious intruders. The web application security scanner accurately scans HTML5, JavaScript and Single-page applications. It can audit complex, authenticated webapps and issues compliance and management reports on a wide range of web and network vulnerabilities.

Features:

Scans for all variants of SQL Injection, XSS, and 4500+ additional vulnerabilities

Detects over 1200 WordPress core, theme, and plugin vulnerabilities

Fast & Scalable – crawls hundreds of thousands of pages without interruptions

Integrates with popular WAFs and Issue Trackers to aid in the SDLC

Available On Premises and as a Cloud solution.

3) Traceroute NG

Traceroute NG is application that enables you to analyze network path. This software can identify IP addresses, hostnames, and packet loss. It provides accurate analysis through command line interface

Features:

It offers both TCP and ICMP network path analysis.

This application can create a txt logfile.

Supports both IP4 and IPV6.

Detect path changes and give you a notification.

Allows continuous probing of a network.

CHAPTER 4

4. IMPORTANCE OF CYBER SECURITY

4.1 IMPORTANCE OF CYBER SECURITY

Cyber security's importance is on the rise. Fundamentally, our society is more technologically reliant than ever before and there is no sign that this trend will slow. Data leaks that could result in identity theft are now publicly posted on social media accounts. Sensitive information like social security numbers, credit card information and bank account details are now stored in cloud storage services like Dropbox or Google Drive.

The fact of the matter is whether you are an individual, small business or large multinational, you rely on computer systems every day. Pair this with the rise in cloud services, poor cloud service security, smartphones and the Internet of Things (IoT) and we have a myriad of cybersecurity threats that didn't exist a few decades ago. We need to understand the difference between cybersecurity and information security, even though the skillsets are becoming more similar.

Governments around the world are bringing more attention to cybercrimes. GDPR is a great example. It has increased the reputational damage of data breaches by forcing all organizations that operate in the EU to:

Communicate data breaches

Appoint a data-protection officer

Require user consent to process information

Anonymize data for privacy

The trend towards public disclosure is not limited to Europe. While there are no national laws overseeing data breach disclosure in the United States, there are data breach laws in all 50 states. Commonalities include:

The requirement to notify those affect as soon as possible

Let the government know as soon as possible

Pay some sort of fine

California was the first state to regulate data breach disclosures in 2003, requiring persons or businesses to notify those affected "without reasonable delay" and "immediately following discovery". Victims can sue for up to $750 and companies can be fined up to $7,500 per victim.

This has driven standards boards like the National Institute of Standards and Technology (NIST) to release frameworks to help organizations understand their security risks, improve cybersecurity measures and prevent cyber attacks.

4.2 Why is cybercrime increasing?

Information theft is the most expensive and fastest growing segment of cybercrime. Largely driven by the increasing exposure of identity information to the web via cloud services. But it is not the only target. Industrial controls that manage power grids and other infrastructure can be disrupted or destroyed. And identity theft isn't the only goal, cyber attacks may aim to compromise data integrity (destroy or change data) to breed distrust in an organization or government.

Cybercriminals are becoming more sophisticated, changing what they target, how they affect organizations and their methods of attack for different security systems.

Social engineering remains the easiest form of cyber attack with ransomware, phishing, and spyware being the easiest form of entry. Third-party and fourth-party vendors who process your data and have poor cybersecurity practices are another common attack vector, making vendor risk management and third-party risk management all the more important.

According to the Ninth Annual Cost of Cybercrime Study from Accenture and the Ponemon Institute, the average cost of cybercrime for an organization has increased by $1.4 million over the last year to $13.0 million and the average number of data breaches rose by 11 percent to 145. Information risk management has never been more important.

Data breaches can involve financial information like credit card numbers or bank account details, protected health information (PHI), personally identifiable information (PII), trade secrets, intellectual property and other targets of industrial espionage. Other terms for data breaches include unintentional information disclosure, data leak, cloud leak, information leakage or a data spill.

Other factors driving the growth in cybercrime include:

The distributed nature of the Internet

The ability for cybercriminals to attack targets outside their jurisdiction making policing extremely difficult

Increasing profitability and ease of commerce on the dark web

The proliferation of mobile devices and the Internet of Things.

4.3 What is the impact of cybercrime?

A lack of focus on cybersecurity can damage your business in range of ways including:

Economic costs: Theft of intellectual property, corporate information, disruption in trading and the cost of repairing damaged systems

Reputational costs: Loss of consumer trust, loss of current and future customers to competitors and poor media coverage

Regulatory costs: GDPR and other data breach laws mean that your organization could suffer from regulatory fines or sanctions as a result of cybercrimes

All businesses, regardless of the size, must ensure all staff understand cybersecurity threats and how to mitigate them. This should include regular training and a framework to work with to that aims to reduce the risk of data leaks or data breaches.

Given the nature of cybercrime and how difficult it can be to detect, it is difficult to understand the direct and indirect costs of many security breaches. This doesn't mean the reputational damage of even a small data breach or other security event is not large. If anything, consumers expect increasingly sophisticated cybersecurity measures as time goes on.

CHAPTER 5

5. CYBER SAFETY

3.1 Cyber safety

Protect yourself against cyberattacks

How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

1. Update your software and operating system:This means you benefit from the latest security patches.

2. Use anti-virus software:Security solutions like Kaspersky Total Security will detect and removes threats. Keep your software updated for the best level of protection.

3. Use strong passwords:Ensure your passwords are not easily guessable.

4. Do not open email attachments from unknown senders:These could be infected with malware.

5. Do not click on links in emails from unknown senders or unfamiliar websites:This is a common way that malware is spread.

6. Avoid using unsecure WiFi networks in public places:Unsecure networks leave you vulnerable to man-in-the-middle attacks.

Related Articles:

What is Cybercrime: Risks and Prevention?

How to Avoid Most Types of Cybercrime

Internet of Things Security Threats

What is Spam and a Phishing Scams?

Related Products and Services:

- Cyber Security for your Home Devices
- Small Business Cyber Security
- Advanced Endpoint Security for SMBs
- Corporate Cyber Security Services
- Cyber Security Awareness Training for Employees
- Enterprise Cyber Security for Industries

CHAPTER 6

6. CONCLUSION

6.1 Conclusion

Depending on their (potential) severity, however, disruptive incidents in the future will continue to fuel the military discourse, and with it fears of strategic cyber-war. Certainly, thinking about (and planning for) worst-case scenarios is a legitimate task of the national security apparatus. However, for the favour of more plausible and more likely problems they should not to get more attention Therefore, there is no way to study the „actual‟ level of cyber-risk in any sound way because it only exists in and through the representations of various actors in the political domain.

REFERENCES

[1]. Daniel, Schatz,; Julie, Wall, (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215. Archived from the original on 28 December 2017.

[2]. Rouse, Margaret. "Social engineering definition". Tech Target. Archived from the original on 5 January 2018. Retrieved 6 September 2015.

[3]. Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.

[4]. "Reliance spells end of road for ICT amateurs", 7 May 2013, The Australian

[5]. Stevens, Tim. "Global Cyber security: New Directions in Theory and Methods". Politics and Governance. 6 (2). doi:10.17645 /pag.v6i2.1569.

[6]. "Computer Security and Mobile Security Challenges". researchgate.net. Archived from the original on 12 October 2016. Retrieved 4 August 2016.

[7]. "Distributed Denial of Service Attack". csa.gov.sg. Archived from the original on 6 August 2016. Retrieved 12 November 2014.

[8]. Wireless mouse leave billions at risk of computer hack: cyber security firm Archived 3 April 2016 at the Way back Machine.

[9]. "Multi-Vector Attacks Demand Multi-Vector Protection". MSSP Alert. July 24, 2018.