Cyber Security

Kumar Shantam

Sofia University

The practice of shielding devices, networks and services from digital threats is cybersecurity. These cyberattacks are usually designed to access, modify or kill sensitive information; ransom users' money; or disruption of normal business processes. Implementing successful cybersecurity measures is particularly challenging today because there are more computers than humans and more creative attackers are becoming.A successful approach to cybersecurity has several protective layers spread through machines, networks, programs or data that one intends to keep secure. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks.

(Retrieved from ‘What is cybersecurity?’ <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>)

During public discussion, cybersecurity is also sometimes incorrectly conflated with other terms such as anonymity, information sharing, intelligence gathering and surveillance. Privacy is linked to an individual's ability to monitor access to information about that person by others. Thus, good cybersecurity may help protect privacy in an online world, but information shared to assist in cybersecurity efforts may sometimes include personal information that some people at least consider private. Cybersecurity can be a means of protecting an information system from unauthorized surveillance and intelligence gathering. Three factors depend on the risks associated with any attack: threats (who attacks), vulnerabilities (the weaknesses they target), and impacts (what the attack does). Risk management for information systems is seen as essential for efficient cybersecurity.

According to Gartner, cloud computing is one of the key drivers for achieving the purpose of an enterprise and is gradually becoming a new norm. As a result, cloud spending will continue to increase, making it the top investment region for businesses in 2019. Cybersecurity is interestingly enough the second major spending factor cited by the CIOs in the same survey. The average cost of a data breach worldwide now equals $3.86 million – $148 per compromised record, according to the Ponemon Institute's recent study. The numbers, however, vary greatly from country to country: from, for example, $7.9 million in the USA to $1.24 million in Brazil. (Retrieved from ‘The Top Cloud Security Threats for Your Business in 2019 and How to Avoid Them’ by Mary Alexandrova, February 2019

<https://easternpeak.com/blog/the-top-cloud-security-threats-for-your-business-in-2019-and-how-to-avoid-them/>)

The top seven cloud computing threats that one should be aware of are:

1. Data Breach: A data breach (or leak) is perhaps the most common concern regarding cloud protection. It generally happens as a result of security attacks on cloud computing, when unauthorized users or programs access confidential data and are able to view, copy, or distribute it.
2. Data Loss: Unlike data breaches, data loss is often caused by natural or man-made events as a result of computer physical destruction or human error. This may also be the product of a targeted attack, though. Regardless of the cause, the outcome will be the same: you lose all the data that you have accumulated for years.
3. Denial of Service (DoS): Another popular type of security attack on cloud computing, a Denial of Service (DoS) attack can shut down your cloud services and make them temporarily (or indefinitely) inaccessible to your users. This can be achieved either by loading the network with heavy traffic, which the servers obviously can not filter, or by making use of the glitches and vulnerabilities to crash it.
4. Cryptojacking: In this kind of security assault on cloud computing, hackers use your computing resources to process cryptocurrency transactions by running a crypto mining script without your permission on your servers. This leads to increased CPU load and can slow down the machine dramatically as a result.
5. Account hijacking: Even if your workers do not use normal, vulnerable passwords, hackers can still "devise" the keys, enter your cloud using the identities of your staff, and as a result steal or exploit your data or otherwise disrupt your business processes. This is named, "account hijacking".
6. Insecure APIs: Even if your own networks are secure, potential cloud security risks can often be added by third-party providers. IoT applications are typically considered a data privacy threat: systems such as smart vehicles, health monitoring apps and home appliances, storing and distributing loads of sensitive data in real time.
7. Insider threats: There are enough internal dangers of cloud computing beyond external security challenges. Of example, your own staff may cause violations of privacy or big leakage of data. This may be because of deliberate criminal activity, or simply because of human error.

(Retrieved from ‘The Top Cloud Security Threats for Your Business in 2019 and How to Avoid Them’ by Mary Alexandrova, February 2019

<https://easternpeak.com/blog/the-top-cloud-security-threats-for-your-business-in-2019-and-how-to-avoid-them/>)

Ransomware is malware that usually enables financial gain from cyber extortion. Within seemingly normal emails or web pages, criminals may conceal ties to ransomware. When enabled, ransomware prohibits users from communicating with their devices, software or programs without paying a ransom, typically in the form of an anonymous currency like Bitcoin. Ransomware is a serious and growing cyber threat that frequently affects individuals and has made headlines for wider business attacks recently. Pay requests range from hundreds to millions of dollars depending on targeted organisations. In recent years the brazenness, popularity, severity and number of ransomware attacks have increased significantly. They include Cryptolocker and its versions including Kriptovor and Teslacrypt, Cerber, Dridex and Locky, and WannaCry, most recently. When ransomware infects the device of a user, it either encrypts critical files or locks out a user from his machine. It then shows a ransom note that normally demands the transfer of virtual currency in return for a cryptographic key to decrypt or unlock certain services. The letter could also risk the public release of corrupted data if the demand for payment is not fulfilled. Any ransomware can migrate to a linked file server or other network hub from one infected device, and then infect that machine. Ransomware's effect is instant, relative to stealthier malware like those used in an advanced threat attack.

Three things must be done to properly defend against ransomware:

1. The intrusion process needs to be thoroughly evaluated to establish the direction of attack and device vulnerabilities.
2. The malicious code needs to be analyzed to determine its intent and indicators of operation (behavior-based analysis).
3. Connection to command and control servers (used for data exfiltration or to access additional malware) from infected machines must be blocked.

This defensive approach relies on connecting warning signs across different vectors that are often overlooked by traditional security solutions. Advanced security solutions, such as [FireEye Network Security](https://www.fireeye.com/solutions/nx-network-security-products.html) (NX Series), [FireEye Email Security](https://www.fireeye.com/solutions/ex-email-security-products.html) (EX Series), or [FireEye Email Threat Prevention Cloud](https://www.fireeye.com/solutions/ex-email-security-products.html) (ETP) stop ransomware from taking control by blocking exploit kits, malware downloads and callback communications to the command and control servers. (Retrieved from ‘Ransomware: The Attacker’s Choice for Cyber Extortion’

fireeye.com/current-threats/what-is-cyber-security/ransomware.html)

Cybersecurity is a dynamic field of study because the threats keep on improving as the technology around us keeps on improving every day. Data has been estimated to be the most expensive asset in today's world. Therefore it is of paramount importance to devise various strategies that point out the threats and then quarantine it accordingly. The protection strategies need to be constantly updated to keep in pace with the technical advancements.

References:

1. ‘Cybersecurity Issues and Challenges: In Brief’ by Eric A Fischer, August 12,2016.
2. ‘Adapting to the new reality of evolving cloud threats’ Cloud security threat report June 2019.
3. ‘Conversational ransomware defense and survival’ by Orlando Scott-Cowley.