Assignment 1

Internet Security

Introduction

Internet security is a catch-all term for a very broad issue covering security for transactions made over the Internet. Generally, Internet security encompasses browser security, the security of data entered through a Web form, and overall authentication and protection of data sent via Internet Protocol. Internet security relies on specific resources and standards for protecting data that gets sent through the Internet. This includes various kinds of encryption such as Pretty Good Privacy (PGP). Other aspects of a secure Web setup includes firewalls, which block unwanted traffic, and anti-malware, anti-spyware and anti-virus programs that work from specific networks or devices to monitor Internet traffic for dangerous attachments. Internet security is generally becoming a top priority for both businesses and governments. Good Internet security protects financial details and much more of what is handled by a business or agency's servers and network hardware. Insufficient Internet security can threaten to collapse an e-commerce business or any other operation where data gets routed over the Web.

Internet security breaches

Viruses, spyware, and other malware

Cybercriminals often use malicious software to break in to protected networks. Viruses, spyware, and other types of malware often arrive by email or from downloads from the internet. For instance, you might receive an email with an attached text, image, or audio file. Opening that attachment could infect your computer. Or you might download an infected program from the internet. In that case, your computer would become infected when you open or run the malicious program. If it's a virus, it could spread to other computers on your network.

Phishing

These attacks work by getting us to share sensitive information like our usernames and passwords, often against normal logic and reasoning, by using social engineering to manipulate our emotions, such as greed and fear. A typical phishing attack will start with an email spoofed, or faked, to look like it's coming from a company you do business with or a trusted coworker. This email will contain aggressive or demanding language and require some sort of action, like verify payments or purchases you never made. Clicking the supplied link will direct you to a malicious login page designed to capture your username and password. If you don't have multi-factor authentication (MFA) enabled, the cybercriminals will have everything they need to hack into your account. While emails are the most common form of phishing attack, SMS text messages and social media messaging systems are also popular with scammers.

Spoofing and session hijacking

TCP session hijacking is a security attack on a user session over a protected network. The most common method of session hijacking is called IP spoofing, when an attacker uses source-routed IP packets to insert commands into an active communication between two nodes on a network and disguising itself as one of the authenticated users. This type of attack is possible because authentication typically is only done at the start of a TCP session. Another type of session hijacking is known as a man-in-the-middle attack, where the attacker, using a sniffer, can observe the communication between devices and collect the data that is transmitted.

Denial of service (DDoS) attacks

A denial-of-service attack is capable of crashing websites. Hackers can make a website or a computer unavailable by flooding it with traffic. DDoS attacks are considered security breaches because they can overwhelm an organization’s security devices and its ability to do business. DDoS attacks often target government or financial websites. The motive can be activism, revenge, or extortion. During an attack, anyone who has legitimate business with an organization like you will be unable to access the website.

But these three examples are just a start. There are other types of security breaches. Cybercriminals can also exploit software bugs or upload encryption software onto a network to initiate ransomware attacks in essence, demanding a ransom in exchange for the encryption key. Or intrusions may occur inside an organization, with employees seeking to access or steal information for financial gain.

How to prevent from internet security breaches

Firewalls

In computing, a firewall is software or firmware that enforces a set of rules about what data packets will be allowed to enter or leave a network. Firewalls are incorporated into a wide variety of networked devices to filter traffic and lower the risk that malicious packets traveling over the public internet can impact the security of a private network. Firewalls may also be purchased as stand-alone software applications. The term *firewall* is a metaphor that compares a type of physical barrier that's put in place to limit the damage a fire can cause, with a virtual barrier that's put in place to limit damage from an external or internal cyberattack. When located at the perimeter of a network, firewalls provide low-level network protection, as well as important logging and auditing functions.

While the two main types of firewalls are host-based and network-based, there are many different types that can be found in different places and controlling different activities. A host-based firewall is installed on individual servers and monitors incoming and outgoing signals. A network-based firewall can be built into the cloud's infrastructure, or it can be a virtual firewall service.

Anti virus softwares

Antivirus software helps protect your computer against malware and cybercriminals. Antivirus software looks at data — web pages, files, software, applications — traveling over the network to your devices. It searches for known threats and monitors the behavior of all programs, flagging suspicious behavior. It seeks to block or remove malware as quickly as possible. Antivirus protection is essential, given the array of constantly-emerging cyberthreats. If you don’t have protective software installed, you could be at risk of picking up a virus or being targeted by other malicious software that can remain undetected and wreak havoc on your computer and mobile devices.

If you already have antivirus software, you may believe you’re all set. But it might not be that simple. With new and savvier cyberthreats and viruses surfacing, it’s important to stay current with the latest in antivirus protection.

If there’s any crack in your cybersecurity defenses, cybercriminals likely will try to find a way in. Ensuring your antivirus software is up and running, and up-to-date, is a good place to start. However, hackers, scammers, and identity thieves are constantly tweaking their methods, so it’s a good idea to get protection from a comprehensive security solution.

Browser Choice

Browsers can have security flaws, which allow hackers and cyber-criminals to attack computers and networks. You must choose a secure browser and keep it updated with new security patches the developer releases. One example of a dangerously insecure browser is Microsoft's Internet Explorer 6 (IE6). Although it's now largely out of use, IE6 has so many security flaws that even Microsoft wants to stop people from using it.

Digital signatures

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. As the digital equivalent of a handwritten signature or stamped seal, a digital signature offers far more inherent security, and it is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence of origin, identity and status of an electronic document, transaction or message and can acknowledge informed consent by the signer.

Digital certificates

A digital certificate, also known as a public key certificate, is used to cryptographically link ownership of a public key with the entity that owns it. Digital certificates are for sharing public keys to be used for encryption and authentication. Digital certificates include the public key being certified, identifying information about the entity that owns the public key, metadata relating to the digital certificate and a digital signature of the public key created by the issuer of the certificate.

The distribution, authentication and revocation of digital certificates are the primary purposes of the public key infrastructure (PKI), the system by which public keys are distributed and authenticated.
Public key cryptography depends on key pairs: one a private key to be held by the owner and used for signing and decrypting, and one a public key that can be used for encryption of data sent to the public key owner or authentication of the certificate holder's signed data. The digital certificate enables entities to share their public key in a way that can be authenticated.

Digital certificates are used in public key cryptography functions; they are most commonly used for initializing secure SSL connections between web browsers and web servers. Digital certificates are also used for sharing keys to be used for public key encryption and authentication of digital signatures.
Digital certificates are used by all major web browsers and web servers to provide assurance that published content has not been modified by any unauthorized actors, and to share keys for encrypting and decrypting web content. Digital certificates are also used in other contexts, both online and offline, for providing cryptographic assurance and privacy of data.

Email Security

Electronic mail (email) offers many potential vulnerabilities. It's often used to send sensitive information, which then becomes vulnerable to theft, and is also used to distribute malware. A solid email security strategy includes both anti-malware applications and good practice by users, such as not sending sensitive information via unsecured email and not opening suspicious messages.

Conclusion

Nowadays internet security is a very important filed. Because the threats are increasing day by day in varies computer fields. Computer security attempts to ensure the confidentiality, integrity, and availability of computing systems and their components. Three principal parts of a computing system are subject to attacks: hardware, software, and data. These three, and the communications among them, are susceptible to computer security vulnerabilities. In turn, those people and systems interested in compromising a system can devise attacks that exploit the vulnerabilities.

From the above report it has been observed what are the internet security breaches in details and how to prevent from those attacks. As discussed we can take many security precautions but the thing is we cannot assure that we are still secure. Because the field of hacking is developing very rapidly. Finally we can say the internet security field is a never ending field until hackers are stopped.