Research paper on preventing hacking in the workplace

Business, Company

With the help of information technology, a company can store vast amounts of data, perform complex operations, and conduct business in a much more expedient way with fewer personnel. However, with that opportuntiy comes risk; computer hackers can wreak havoc on a business' network, leading to stolen information, corrupted data, and compromised business. If a company does not take appropriate steps to guard their networks, they can fall prey to all manner of hacking attempts. Luckily, there are detailed and comprehensive steps you can take to secure your information and maintain an information secure workplace. With the help of high-bit encryption, password-protecting, authentication and zero-knowledge proofs, a company can successfully guard against even the most skilled hackers.

When a system is hacked, a cyberattack occurs on the part of someone who infiltrates an outside network and accesses the information in their databases. These are forms of computer crime, and it can lead to classified information being leaked, insider information being sold to other companies or used for the hacker's own personal gain, or blackmail, both personal and corporate. In the event this was to occur, entire companies could be taken down – as a result, the most thorough precautions must be taken. Crimeware is " the blanket term for code aimed at garnering cash," and it can strike companies at any time if they are not prepared (Lemos, 2006, p. 117).

The US government has acknowledged cyberwarfare as something that can threaten national security; as a result, they take steps to plug whatever holes they can. There are even active algorithms that seek out potential attacks, anticipating them before they occur. Real time sensors can " detect

and stop malicious code” before it passes into the network (Lynn, 2010). While this may be out of the reach of a corporate environment as yet, there is the possibility for it becoming available in the future.

Network firewalls are a company’s first line of defense against hackers. This involves a comprehensive network of security measures designed to keep out anyone who isn’t allowed to access this information. This can take the form of encryption, authorization, and many other methods. Any and all applications that are used in the workplace (office programs, Internet browsers, and the like) must be walled off with security programs. Provided “ patches” are installed to your firewalls as they come out, you can plug any holes that can be used by hackers to get through (Morgan, 2006).

One way in which hackers can get into the network is through a lack of encryption on said network – information over routers and servers are transparently transported from one place to the other, and anyone on the Internet service provider (ISP) can access that information. However, encryption allows all information on this router or server to be scrambled and encoded, to be deciphered on the machine itself when it is successfully transmitted. This way, it cannot be intercepted by an outside party. The higher the number of bits are in your encryption algorithm, the more complicated the encryption is, and the less likely it is that a hacker could decrypt it. 64-bit encryption is normal for consumer encryption, but 128, 194 and 256-bit encryption provides a reasonable level of protection against hackers. There are even 2048 bit SSL certificates that can provide even further protection (Lysyanskaya, 2008).

Secret key systems and public key systems are also very effective varieties of encryption that can help stave off hackers. With a secret key system, all employees have a secret key that must be used to encrypt and decrypt messages. Public key systems still use secret keys, but a public key can also be used to encrypt - the secret key must be used for decryption, however (Lysyanskaya, 2008).

It is one thing to encrypt your data; how does the employee receiving the message know that it comes from the person it claims to? Hackers often use this strategy, known as phishing, to pretend to be someone else in order to get them to reveal information that can be stolen. However, with the help of authentication of your messages, it can be rendered safe to communicate with employees between terminals. This also uses the secret key/public key system, wherein a digital signature is created to verify the person who sent the message. The secret key is used to encrypt the message and send it to the recipient, who uses their own key to decrypt it – the sender's public key is compared to the decrypted secret key; if they match, the sender is verified (Lysyanskaya, 2008). This makes it easy to detect fake phishing messages, as the keys would not match up; what's more, it is impossible to forge, as the secret key is necessary to create the digital signature.

Obviously, protecting your router with a password is the simplest action you can do to protect your computer from invasion, and this applies to a workplace environment as well. Having both individual, employee-related passwords for their terminals and secure passwords to access router/server settings is a good idea. Employees must be given or encouraged to create

strong passwords that include both upper- and lower-case letters, numbers, and special characters. It must also be a password that the employee does not use for anything else, or nothing that is related to their birthday, family members, or anything a hacker could guess, particularly if they know the person in question (Lemos, 2006).

Another simple but extremely effective step is to make sure all system and Internet browser updates are performed. New hackers are finding new loopholes to existing technology every day; as a result, it is necessary to follow through with new updates to all terminal operating systems, email programs, Internet browsers, and antivirus software. Internet browsers improve their security all the time to ensure that new viruses and security gaps are accounted for; create a consistent weekly (or daily) schedule for all employees and IT personnel to actively update computer software and router firmware (Lemos, 2006).

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are two varying kinds of security algorithms used to protect a IEEE 802. 11 wireless network from hacking. With the help of either of these algorithms, it is incredibly difficult for a hacker to access router settings or the stations hooked up to it. Currently, WPA is the preferred method of security check, due to its improved encryption abilities; therefore, adding that protection to your wireless network can additionally guard the network from a hacking attempt.

When encrypted messages are sent from terminal to terminal, one issue can be whether or not the person providing the message is legitimate. At the

same time, the sender does not want to acknowledge the subject of the message, as that can reveal to a hacker who intercepted it the reason for the message. However, anonymous authorization scenarios require employees to have secret keys (SK), unique signatures that can be sent back that verify their identity without actually revealing them or the contents of the message. This is a way to weed out potential phishers, and stop hackers from pretending to be a part of the company to get information. The employee could also interact with the Internet without revealing who they are, or linking their behavior to anything that could be traced back to the company (Lysyanskaya, 2008).

Onion routing takes encryption to the next level – when an employee sends a message to another, they can provide multiple layers of protection and encryption on it, with a public key (PK) from multiple people on each layer. This message can then be sent down the chain, each different employee unpeeling their own layer with their PK, until it gets to the real recipient, who can then decrypt it fully and get the message they want (Lysyanskaya, 2008).

One very effective strategy for keeping out hackers is eliminating access to the Internet altogether. Intranets and extranets are extremely viable alternatives for keeping information within a localized network of computers. No outside access to the Internet means that no one can get in without accessing the local stream itself. All terminals are connected through wires to the server, and no one can connect wirelessly. In the event you have a computer network that does not need to access anything outside that physical space, this can most definitely work for your company. This creates

an insular bubble that is impenetrable to anyone who is not physically within the building and accessing a terminal plugged in via wire to the server or router.

Despite all the technical measures taken to reduce the chances of being hacked, nothing provides a greater level of protection than vigilance on the part of employees. Training and communication regarding avoiding spam websites, banner ads, and popups are the most important way to keep your employees from sabotaging themselves and the company. All it takes is for one single employee to click on a popup ad they shouldn’t have to let a hacker release a Trojan or virus into the system. With this in mind, be sure to educate employees on

In conclusion, there are a number of things a company can do to prepare a workplace to defend against hacking. Employees must remain vigilant and exercise best practices in avoiding spam or viruses. Computer software and firmware must constantly be updated for the newest versions and protections. 256-bit or greater encryption must be used for routers and servers on your network. Authentication algorithms must be chosen with care and in great detail; a secret key/public key system is a very good way to transmit messages without risk of phishing. Onion routing allows information and messages to be confirmed or communicated about without anyone looking in, and anonymous channels protect the identity of recipients of messages. If all of these measures and more are taken to prevent corporate hacking, the information contained within the network can remain safe.

References

Lemos, R. (2006). Hacking for Dollars. PC Magazine, 25(23), 117. Retrieved from EBSCOhost.

Lynn III, W. J. (2010). Defending a New Domain. In , Foreign Affairs (pp. 97-108). Foreign Affairs. Retrieved from EBSCOhost.

Lysyanskaya, A. (2008). HOW TO KEEP SECRETS SAFE. Scientific American, 299(3), 88-95. Retrieved from EBSCOhost.

Morgan, R. (2007). Essential Security: Firewalls. PC Magazine, 26(10), 91. Retrieved from EBSCOhost.