

Instant Messaging and P2P Vulnerabilities for Health Organizations

Because of HIPAA legislation, health organizations have to be particularly careful about the vulnerability of the patient data they maintain. Exposing patient data to the Internet through IM exchanges or P2P file sharing can jeopardize their compliance with a variety of state and federal regulations. The popularity of IM and P2P protocols has penetrated every aspect of our society including those organizations entrusted with sensitive data such as health records. The opportunity for data to be exposed to eyes outside an organization has increased whether such exposure is intentional or not and organizations bound by HIPAA regulations are required to protect their patient data or suffer the consequences. Often in hospital situations, employees on different shifts are sharing workstations. Many of them may be communicating with family and friends, outside the organization, via Instant Messaging or P2P and can unknowingly download a malicious agent that can damage not only individual workstations, but entire networks. Because many people may have access to the same computer, this activity is difficult to trace and can occur with alarming ease. When a malicious program is downloaded, it can exploit a back door in the system and proliferate across the network. Depending on the nature of the parasitic code, patient information may be accessed and transmitted from behind the firewall to a designated IP address or it may launch an attack against the host network. These types of attacks can bring the network down. Even short downtime can cause significant financial and data loss.

Public Communications

Adding more complexity to the situation, the Securities and Exchange Commission (SEC) and the National Association of Securities Dealers Inc. (NASD) identify Instant Messaging traffic as communications with the public that companies must save and monitor. The Sarbanes-Oxley Act requires even those instant messages that are casual and personal to be saved and recorded as formal correspondence. Many companies capture and store the data as required by law. Because this information can be used as legal evidence, there are several instances where data contained on message boards and via IMs were submitted to support or defeat a case being adjudicated. Imagine if medical advice were contained in an IM, even something as innocuous as advising Tylenol for a feverish child. Such correspondence could be used to make a medical malpractice case against a nurse or physician.

Network Security

IM and P2P also expose end-user equipment to worms, viruses and other backdoor software that -once introduced, can infect a network and inflict damage on a wide scale. Employee abuse of their computer privileges can be the silent destroyer of networks. Whether it is a dramatic problem such as denial of service or the downloading of backdoor worms and viruses, the misuse can be dangerous and damaging and ultimately undermines network security. Managers of network security need to take advantage of hardware appliance solutions in order to fully protect their networks from employee abuse and misuse. The damage to productivity and profits of a company are only the tip of the iceberg. Introducing a filtering option that does not have a single point of failure, or cause latency in network traffic is critical. Equally important, a solution that doesn't need to share memory or processing power with another device is the best choice to protect networks against security breaches and legal liability and to help preserve the corporation's good reputation.

Legal Liabilities

P2P and IM file sharing can be dangerous applications that quickly devour bandwidth and jeopardize company finances because companies can be held liable for employee actions such as downloading copyrighted song material. In addition, P2P and IMs can contain malicious software that downloads and installs itself into the host network; a company's computers and networks may be used to launch denial of service (DoS) attacks on other companies and networks. There is an established legal precedent that will hold a company liable in part for the damages inflicted on another company if their computers or networks were used to stage the attack. Because of this legal precedent, the danger to a host network is not just the loss of bandwidth and subsequent breakdown in communications, but also the legal liabilities involved can result in damage to a company or organization's reputation, and even threaten its financial stability. It's important to note that the damage to an organization's reputation can be more costly in the long run, especially if the organization is supposed to be secure and web savvy or if security vulnerabilities can threaten to expose sensitive data such as health records. For hospitals, health insurance and dedicated health care providers, such damage can result in a loss of business over time that devastates their long term prospects and when combined with -short term fines, can even mean going out of business or experiencing a takeover by another health care company.

About the Author

In oriental medicine there are many different reasons why you can experience migraines. Help us improve Yahoo! Answers. Tell us what you think.

Source: <http://www.productsherbal.com>