What Every VAR Should Know About Email Security

Following these key tips will go a long way in protecting your customers from email-borne security threats.

By Andrés Kohn, VP of technology, Proofpoint, Inc.

The Internet has become more treacherous than ever in the twenty-first century. The vision of a lone hacker operating out of a basement is hopelessly out of date. Today, a well-organized data theft industry exists, complete with hierarchies, well-defined roles for participants, and established global supply chains. Employee behavior can play a major role in defeating the data theft industry, and therefore education is crucial. There are two times when employees should exercise special care: when they receive or send email, and when they access the corporate network, whether for their email or an application.

Email: Inbound Threats

Email is the fundamental mode of communication in today's business world, and as such is a wide open path into the depths of an organization. This also makes it the launch pad for enormous volumes of malware or phishing messages and recently, an alarming number of targeted attacks. These sophisticated "spear phishing" attacks target executives and high-level IT managers with cleverly disguised messages that often appear to have come from a friend or co-worker and contain personal information (often gleaned from a social network) that further creates an impression of authenticity. They also contain links to malicious URLs that enable the theft of network credentials or the surreptitious download of malware, allowing cybercriminals to gain a foothold that leads to the eventual loss of everything from intellectual property to clients' personal information such as credit card and personal identification numbers.

Employees need to be trained never to click on suspicious links. In the era of spear phishing, this is not an easy task.

Email: Outbound Risks

A second threat is the loss of data contained in outbound email. While email may feel like a private one-to-one communication, employees need to understand that it is in fact no more private than a physical postcard. As such, it is critical to implement easy-to-use email encryption solutions to secure communications, and then train employees on which types of data should never be sent in email unless it is encrypted. Employees should also not request sensitive information via email, thus encouraging customers or vendors to break the rules and perpetuating this problem.

Andrés Kohn

proofpoint

Andrés Kohn is the VP of technology at Proofpoint, Inc., a security-as-a-service vendor that delivers data protection solutions to medium- and large-sized organizations.

Network Access — and Vulnerability

Two huge IT trends — mobility and consumerization — have combined to pose serious new security threats. The universal adoption of mobile devices for business means that large numbers of employees routinely access the corporate network from cafés, airports, and other unsecured wireless networks. This is in itself a risk — and consumerization means employees often take this risk while using devices that don't provide the levels of security appropriate for business. Worse, these devices are frequently shared with other family members on evenings and weekends, exposing them to a plethora of attacks. Employees need to understand the risks of using unsecured networks, observe a strict "division of labor" between office and home devices, and, use strong passwords on every device.

Passwords

Passwords are an important component for combating data theft, and employees should be trained to use passwords. Also, employees should understand that passwords like "123456" or "password" are no better than no password at all. Also, names of pets or other pieces of information that might be found on a Facebook page should be avoided. At minimum, passwords should have at least eight characters, including letters, numerals, and a non-alphanumeric symbol like & or %, and be changed on a regular basis.

A Technology Safety Net

By following the best practices outlined above, malware or targeted attacks embedded in inbound email can be blocked with extremely high capture rates, and outbound email can be filtered to block or selectively encrypt messages containing sensitive data. Companies can also limit access to the corporate network and enforce password policies.

Employees aren't perfect. In any situation where sensitive data is involved, IT managers should evaluate security technology regularly to make sure employees have the extra security support they need. ●

Web Exclusive