Network Security for 3PL and Trucking Companies: Simple Concept, Complex Reality

By Chuck Cook, RenovoData

The objectives of good security systems could not be simpler: protect networks from attacks. In practice, these systems are as complex as the networks they protect.

For a security system to be effective, it must protect every area of the network, from servers to minor applications. Coverage needs to be as strong and thorough as possible in every area.

Not only do the technological components need to be safeguarded, everyone who works with the network needs to be shielded by a well-planned set of security procedures.

Setting up and maintaining top-notch security capabilities takes time, often an unpredictable length of time, and that can be especially challenging for 3PL and trucking companies. In addition to time, getting security right requires extra effort and cooperation across the organization, but the results can be the difference between a company's success and potential collapse.

Security-risk lingo

Any network can have weak spots that can be penetrated by malware. These weaknesses are known as vulnerabilities, and it is the job of security to eliminate or diminish them.

There are technological creations traveling through cyberspace that are intended to damage or destroy networks and the data they contain. These are called threats.

When threats attempt to break into networks—when they assault fortress walls—they become attacks.

When attacks succeed in entering networks, they create breaches, intrusions which can be anything from annoying Facebook hacks to the destruction of major governmental capabilities.

It is all business and it is all technology

When planning a security program, the concerns of nontechnical management should be part of the process. Again, this requirement can hit 3PL and trucking companies harder than most businesses. Quite often, management expectations and IT capabilities do not match very well, and conflicts can easily arise. As a matter of policy, management wants speed. But as IT installations become more complex, activities such as security planning can become progressively slower, causing pressure from upstairs that can harm the outcome. In developing network security programs, business and technical people need to reach clear agreements with regard to the requirements, specifications, time, and expense involved.

Another cost is the toll on employees, who may feel that security implementation is a heavy and unneeded pressure that impairs their performance. Finally, from both management and employee perspectives, security implementation uses crucial technical resources without creating immediate tangible value.

Solving people problems in advance

To lay out the details of the security plan and to head off any confusion within the organization, it is necessary to create a document that defines the entire security system in considerable depth. It includes technical specifics, from the firewall to the smallest apps. It explains how operating systems, servers and data are to be secured, how system updates happen, how files should be configured, how jobs are to be run, and much more.

If it is thorough, the document will be long and detailed. To be continually effective, it must be updated to reflect changes within the network and should be reviewed quarterly.

One of its main goals is to reduce human error by making all concerned personnel part of the security process. Human error is central to disasters, largely because people do not realize how much damage a careless action can cause. Such seemingly harmless acts as opening an apparently unimportant email, sloppy handling of passwords, or accidentally releasing critical information can spell calamity.

Problems like these—both human errors and resentment about the intrusions caused by creation of a solid security process—can be greatly reduced by the implementation of ongoing training. A well-planned training program teaches the details of the company's safety procedures, as well possible consequences if they are not followed.

What to protect

Servers, switches, routers, hubs, and other main hardware components are not usually thought of as points of entry for threats, but they can be, so it is

Continued on page 26

important to stay abreast of the latest firmware to minimize vulnerabilities. These infrastructure components should always be included in planning and testing processes.

User devices, such as laptops, tablets, smartphones and USB drives, can become highly vulnerable endpoints as soon as they are connected to the network. Any of them may contain hidden infections, so their network access should be carefully restricted. Any number of endpoint security products are on the market, so every device can and should be protected.

Any application might have flaws that could be exploited by hackers, who understand the vulnerabilities of many software products. This is especially true if older versions have not been deleted from the system, so simply installing a new edition may not be helpful. Also, using the same operating system for all of the organization's computers raises the possibility of threats that can enter through one component to spread more rapidly to others.

Know your enemies

There are two species of villains.

Inside hackers are people who have or have had access to the network. They are likely to be current or former employees and their motives may be grudges, theft, or political mischief. The best defenses against these vandals are good recordkeeping and employee vigilance.

Outside hackers possess professional-level skills. Some of these people simply enjoy acts of cybervandalism, while others, like perpetrators of ransomware, are after money. Some are neurotics who hole up in their basements and others are prosperous criminal entrepreneurs. Outside hackers may use accomplices within the organization.

Know their weapons

Like hackers, threats come in two categories: structured and unstructured. Skilled hackers create structured threats built on their knowledge of network design, current security technology, network access methods, hacking techniques, and custom scripting and applications. Structured threats can be the work of lunatics, terrorists, spies, corporations, or governments, and any institution, government or organization is at risk. The recent hack of the Democratic National Committee is a prime example.

Strong nominees for Public Threat Number One are advanced persistent threats (APTs). These are exceedingly complex multi-component structured threats that stealthily penetrate and corrupt networks over long periods, so that the damage is hard to detect until great harm has already been done. The Chinese and Russian governments are good at making and launching APTs.

Although unstructured threats are far less ominous that the structured variety, they can inflict severe damage and are to be feared. Some are aimed at specific targets while others are fired into cyberspace and can land on random victims. Unstructured threats are cobbled together with readily available tools, and often contain odd characteristics that hackers insert to make their malware harder to fight.

Testing, testing, testing

Security experts agree that the most powerful and effective defense is frequent and thorough testing. Fortunately, regularly scheduled testing is on the rise. Recent studies suggest that up to 40 percent of organizations test at least once a year, and upwards of 30 percent do so at least twice a year.

How often should companies perform security testing? Its value is indisputable, but the interruptions it causes indicate that there is an optimum number, and that it varies between companies. It is likely that 3PL and trucking companies encounter significant resistance, but benefit from pressing ahead. Ultimately, the decision to evaluate your company's security posture is up to you.

For more information on overall data and systems protection for 3PL and trucking companies, please reference RenovoData's website at www.renovodata.com or call 1.877.834.3684