Security Risk Analysis Basics For Solution Providers

20 Jun 2008 | SearchSecurityChannel.com

By Steve Bigelow, Features Writer

No matter how much effort and resources go into securing IT infrastructures, businesses still face a wide range of risks as a result of threats and vulnerabilities like configuration errors, intrusions, viruses and even employees themselves. Corporations are rarely skilled or objective enough to perform thorough evaluations of their own security strategies, so solution providers can step in to perform a security risk analysis -- a detailed investigation that examines every aspect of the client's security posture, identifying weaknesses and recommending corrective actions. The first installment of this Hot Spot Tutorial introduces the basic concepts of threats and risk and the essential elements of a security risk analysis for solution providers interested in offering this service.

Understanding risks and threats for security analysis

The basic goal of any security risk analysis is to understand the client's risks and vulnerabilities and to determine the various realistic threats from inside and outside of the organization that can exploit those vulnerabilities. While the terms "risk" and "threat" are often used interchangeably, some solution providers are quick to emphasize a distinction between the two.

"There's a fairly finite number of risks that actually impact an organization," said Andrew Plato, president of Anitian Enterprise Security, a security solution provider in Beaverton, Ore. "Threats, on the other hand, are numerous and expansive …virtually limitless."

Security risks and threats can be categorized many different ways, but often involve some mix of viruses, spyware, worms, intrusion (or other external attacks), inadequate OS or application patching, device control oversights, firewall configuration mistakes, access control problems and hardware faults. For example, your client may rely on a mission-critical database for everyday operation. The data might be at risk for theft due to vulnerabilities including unpatched operating systems, improper intrusion detection/prevention and inadequate device controls.

So what are some common security business risks? IT personnel often choose to consider issues that are easy to quantify: viruses, intrusions, unauthorized devices on the network (such as USB thumb drives) and other technical threats. These are certainly important, but it's the people within an organization that pose the biggest risk. People are hard to control, and the levels of trust allotted to employees make them able to circumvent many of the routine precautions implemented to guard against outsiders.

"If you look at … the significant intrusions and events that have occurred over the past few years, you can trace almost all of them back to a person or human error," Plato said, noting common oversights like configuration errors, failure to follow established processes or even employee ignorance about security. The underlying message here is that any security risk

analysis should include a thorough evaluation of the client's employees and their roles, permissions and access rights.

Other solution providers note an overall sense of malaise pervading their client organizations, allowing routine security tasks like patching to fall by the wayside. "It's not the evil geniuses that get you," said Wade Wyant, managing partner at ITS Partners LLC, a Symantec consultancy headquartered in Grand Rapids, Mich. "It's the stupid errors, and [businesses are] making so many of them." Many security solution providers are stepping in to fill the security gaps left by overworked, understaffed IT organizations of all sizes.

Effect of changing threats on security risk analysis

Solution providers must understand two important principles in today's security landscape. First, threats are becoming increasingly sophisticated. Second, throwing more technology at these threats is not always the best solution. It's more important to select the proper tool for the corresponding threat, configure each tool properly, and then employ those tools correctly and consistently -- factors that are often overlooked in today's busy IT environments. When performing a security risk analysis, consider if and how security technologies are employed in your client's environment.

Security precautions should also match the risk presented by each network user. Individuals are quickly learning that the easiest way to steal data or perform other malicious acts against a company is to take an entry-level position -- perhaps as a help desk technician -- gain rights within that organization, and then simply exploit the company from inside: stealing information, installing malware and so on. Consequently, a comprehensive security risk analysis should closely examine access controls and user rights throughout the client's organization.

This people problem also extends to trusted partners and other outside users with rights to your client's network. A common example is outside suppliers that access the client's corporate network for just-in-time deliveries or shipping. "Your perimeter walls are going away," said Allen Zuk, senior consultant with GlassHouse Technologies Inc., an independent IT infrastructure consulting and services firm in Framingham, Mass. "More often, clients are allowing their suppliers and channel partners access to their back end."

Improper security precautions may allow those trusted partners to access more information than they should. Similarly, their own inadequate security precautions can jeopardize your data if it resides with the partners. This is another place where a thorough security risk analysis can reveal potential gaps in the client's security.

Today's remote workforce poses another significant threat to network security -- a growing problem even for small businesses. Laptops with sensitive data can easily be stolen, so organizations are challenged to protect mobile systems with technologies like backup and encryption. Laptop users also stray out of the network environment, exposing the unit to threats in the wild. Check to ensure that clients are using network access control, device control and other emerging features found in today's integrated endpoint security suites.

One last factor that affects threat identification and remediation is time. Several years ago, a threat such as a worm might take days to propagate, and security experts had time to study the threat and prepare a response. Now significant propagation occurs in a matter of seconds -- the threat and its impact on the client are almost simultaneous. These "zero-day threats" must be identified and accounted for almost immediately. A security threat analysis should include an evaluation of response/remediation times.

Essential areas of security risk analysis

There is no one right way to perform a security risk analysis -- the means of collecting data and presenting results are as varied as the solution providers that perform them. But experts are clear that simply scanning for vulnerabilities or viruses is not enough. "A lot of companies think that running scans of servers and workstations is synonymous with a security risk analysis, which it is not," Plato said. "You can scan a network until the cows come home and you'll still have very little insight into the actual security of that organization."

While some solution providers adopt standardized security test protocols such as ISO 17799, the ultimate goal in security analysis is to achieve a complete and objective understanding of the client's entire security position. This involves testing and evaluating every security aspect of the network and the greater organization, and often breaks down into several key areas.

Start with the basics. A security risk analysis normally starts by checking the client's defense against basic threats such as viruses, spyware and other known malware. Inadequate defense often requires separate remediation recommendations to update the underlying security software and ensure the latest definition files. An analysis then employs vulnerability testing tools to scan operating systems and key applications throughout the network for appropriate patch levels. Patching vulnerabilities can prevent hackers from leveraging exploits in network software.

Network rights and access controls must also be evaluated for users both inside and outside the organization. Rights should be aggressively limited based on roles and positions within the company. Investigate external access through company Web portals, remote access from mobile employees and other avenues.

Spend time evaluating the mechanisms used to detect and prevent intrusions. Examine the configuration of firewalls and intrusion detection/prevention software or appliances to ensure that they are guarding against appropriate threats, but don't stop there. "Set up traffic analysis reporting," Zuk said. "Establish baselines of what my typical traffic would be for the organization, and then flag against anomalies." Study device logs and traffic patterns to see how security devices respond to various external and internal events.

Don't overlook the importance of client cultures and established policies related to security. Study the people and see how they interact with each other and between business units. "Companies that have a strong internal culture can often overcome a lot of technical and policy and procedure weaknesses," Plato said, noting that, conversely, poor cultures can undo even the most sophisticated security precautions. Also study the client's security response and remediation procedures to see how they actually respond to threats when they occur.

Security risk analyses are rarely one-time endeavors. The results of periodic analysis can often be used as waypoints that help an organization maintain a proper security posture in the face of changing threats, technologies and corporate cultures. The client often opts to use a separate solution provider for any corrective action, but comprehensive solution providers sometimes handle remediation, as you'll see in the third installment of this Hot Spot Tutorial. But first, stay tuned for our second installment when we look at tools and practices for performing a security risk analysis.