Survey Shows Organizations Have Plenty of Room for Improvement with IT Security

No one needs to convince senior executives that a strong information security strategy is of vital importance to businesses. Recent high-profile security breaches have reminded everyone of the need to be diligent about security. And the significance of enterprise networks, systems, applications and information to the day-to-day operations of organizations makes protecting those IT assets a high priority.

Despite the need for robust security, many companies find themselves woefully unprepared for attacks. A new report from IDG Research Services, sponsored by HP, shows that many organizations lack confidence in their ability to sufficiently provide information security.

The study also shows that many companies are not taking advantage of tools such as sandboxing technology, much less integrating the technology so that it works with their network security solutions to detect and block attacks. They also lack the ability to quarantine once they've been hit. Finally, organizations are taking far too much time and too many steps to discover and mitigate breaches, the research shows.

By leveraging the latest security solutions on the market, enterprises can defend themselves against advanced threats and targeted attacks to run more efficient security operations.

NETWORKWORLD
Custom Solutions Group

SPONSORED BY:

Security: A Major Challenge for Enterprises

Countless technology trends have come and gone over the last two decades, but one thing that never seems to leave the IT management radar screen is information security. And with the increasing sophistication of attacks, the growth of mobile devices and social media, and the emergence of cloud services as key components of IT strategies, it's arguable that there has never been a more important time to have effective security in place.

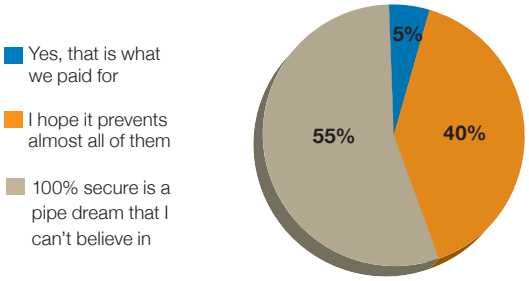
"The attack landscape has indeed become highly sophisticated; in effect, a multilayered and overlapping marketplace of threats and bad actors that progressively amplifies the quality of its weaponry, targeting effectiveness and delivery means," says Anthony Woolf, director of product management for HP TippingPoint.

"The only viable response is to provide a similarly sophisticated layered approach with countermeasures in place in case an attack successfully eludes your first or second lines of defense," Woolf says.

Industry research shows that security breaches can be costly, not just in terms of lost or stolen data, but threats can stick around for months, costing businesses millions of dollars. In fact, the Ponemon Institute has said it takes 243 days to detect a threat once it is in your network.

There can also be damage to corporate reputations and loss of customer trust. Recent attacks on well-known companies have reinforced the idea that businesses—and their customers—are vulnerable.

Virtually none of the respondents believe with any certainty that their current network security solutions will prevent all potential security incidents. If fact more than half think that 100% secure is a "pipe dream".



Do you expect that your current network security solutions will prevent all potential security incidents?

Source: IDG Research, November 2014

According to CSO's annual "State of the CSO" report, which surveyed 366 security professionals online in August and September 2014, about half of the survey respondents say their organizations have had to reevaluate their information security standards as a result of recent well-publicized attacks.

Much work needs to be done. The IDG report, which surveyed 66 IT, security and business professionals in October 2014, shows that only 5% of the respondents think with any certainty that their current network security solutions will prevent all potential security incidents. More than half (55%) say 100% secure networks is a "pipe dream," and the remaining 40% say they can only hope that their security solutions can prevent almost all of the attacks.

"For years, vendors have talked about silver-bullet methods to stop attacks, with customers only now coming to realize the full complexity of the threat landscape and the need for a layered approach," Woolf says. "The reality is that it's just a matter of time before someone successfully penetrates a given organization. The real question is what are you going to do when that happens? Do you have a comprehensive malware detection tool to help identify advanced threats in your network? Do you have the systems in place to neutralize the first infected host—patient zero? Do you have a comprehensive solution to provide continual intelligence to your security operations center?"

Only one-third of the organizations surveyed report that their network security solution, such as a firewall or intrusion prevention system (IPS), can "see" the infected system and automatically quarantine the host. In most cases, companies do not have the means to quarantine the host immediately or in an automated way.

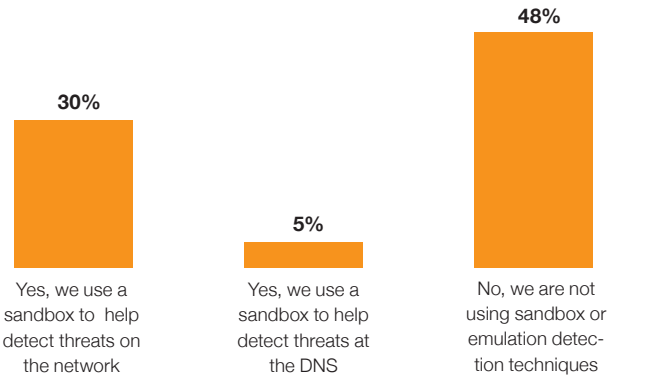
Nearly one-quarter of the organizations (23%) do not quarantine the host at all, opting to pull the system offline in the event of an attack. Without the ability to automatically quarantine an infected host, a threat such as malware can quickly spread through an organization, causing far more damage than if it were stopped early on. In addition, there will likely be a loss in productivity among IT staff and business users.

One potentially effective way to isolate security threats within a network early on is to use

sandbox tools. But only 35% of the survey respondents say their organization uses sandbox or emulation detection techniques to help detect threats on the network or at the domain name system (DNS). It's important not only to have sandbox tools, but that they communicate with intrusion prevention systems and next-generation firewalls to control threats quickly and prevent future attacks.

Just one-third (35%) use a sandbox to help detect threats on the network or at the DNS

Are you using sandbox or emulation solutions to detect threats in your network?



Source: IDG Research, November 2014

Companies certainly have the need for technology tools that can help them detect and address security threats quickly. The survey shows that nearly half of the respondents (48%) report that their organization's process for identifying the initial target of an attack involves several steps.

Four in 10 say the process takes days, weeks or even longer. The delays in detecting and resolving security threats can not only lead to higher costs and growing frustration within the workforce, but there is a greater likelihood that the threats will result in a drain on IT security resources and damage to the business.

"Our internal mantra is 'every second matters,' which is our way of saying that organizations under continuous attack need a defense system that operates at hyper-efficient speeds," Woolf says. "In a layered approach, the IPS must screen [more than] 99.99% of the incoming attacks to allow security professionals to focus on advanced threats that come in through email, downloads or even USB sticks. The role of any IT security team should be to eliminate as many steps as possible and do it as quick[ly] as possible."

Organizations are a mixed bag when it comes to security vendor strategies. Thirty-eight percent say having more vendors means better protection. But nearly the same percentage of respondents (33%) prefers to use a single vendor for simplification. Another 30% have no preference.

The fact is, while having a single vendor certainly removes complexities, many organizations rely on more than one security technology provider. A key factor in selecting a vendor, therefore, is whether the company's products can be easily integrated with those of other providers, and how well the vendor understands supporting a multivendor security environment and the importance of working with partners in the industry.

Solutions Combine Protection with Efficiency

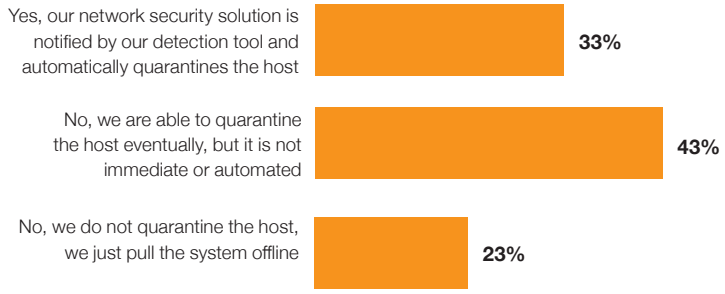
Some of the latest security solutions on the market address many of the challenges organizations are facing when it comes to identifying threats quickly and resolving them effectively.

For example, HP is offering the TippingPoint Advanced Threat Appliance (ATA) family, which provides a comprehensive set of network and mail detection capabilities to detect advanced network threats using multiple detection techniques.

By allowing suspicious files or malware to "detonate" in a safe sandbox environment the HP TippingPoint ATA can analyze the threat and communicate with the HP TippingPoint Security Management System (SMS). This allows for simple remediation and blocking by alerting the HP TippingPoint Next-Generation Intrusion Prevention System and HP TippingPoint Next-Generation Firewall.

Just one-third (33%) report their network security solution is able to see the infected system and automatically quarantine the host. In most cases, companies do not have the means to quarantine the host immediately or in an automated way

Once an infected system is identified, is your network security solution (e.g., firewall and/or IPS) able to see the infected system and automatically quarantine the host?



Source: IDG Research, November 2014

These key components of the HP TippingPoint solution can learn and stop malware and other threats before they can spread within an organization. Working together, the TippingPoint components analyze and detect advanced threats as well as stop the threats at patient zero, keeping the threat from moving laterally through an organization.

Using a set of automated blocking techniques combined with advanced threat detection and analysis, the HP solution provides organizations with an enhanced defense against advanced threats and the subsequent lateral spread. All of this is backed by HP Security Research and the Zero-Day Initiative, which researches vulnerabilities to make sure organizations stay on top of the latest threats and have virtual patches for any vulnerabilities found.

Organizations are facing perhaps the biggest challenges ever when it comes to information security, and many are clearly not prepared. Current solutions and techniques can lead to long delays in finding and mitigating security threats—which can be disastrous from a business standpoint.

Solutions such as those offered by HP enable companies to address targeted attacks quickly and effectively before they get out of hand, using advanced threat detection in conjunction with firewalls and IPS tools.

Although the need for better security is well known among senior business executives today, IT and security leaders need to take the lead in pushing for stronger security within their organizations. The stakes are too high to settle for modest security efforts.

The tools are available to help improve security posture. It's just a matter of putting the right pieces together to provide a simple and effective solution to what has become a complex business challenge. ■

For more information about HP TippingPoint, visit **hp.com/go/tippingpoint.**