Commentary

Diversity Increases Security in Desktop Computing

In enterprise computing, similar to nature, a diverse environment is more resistant to "infection." Enterprises hit by SQL Slammer and MSBlast should consider the security benefits of using more than one desktop operating system.

The most-effective enterprise security strategy is preventing attacks by selecting, developing, deploying and maintaining systems that eliminate or shield vulnerabilities. However, anything that can go wrong will go wrong, and the majority of computer systems will experience some level of intrusion at some point. You also must take action to limit the impact of successful attacks. Supporting diversity of operating systems, especially on the desktop, has numerous security benefits — but it comes at an operational cost. For many enterprises that were damaged by the SQL Slammer and MSBlast worms, the benefits of moving some groups of users to diverse operating systems will outweigh the cost.

The recent upsurge in malicious-code attacks that target Windows, which is used on more than 90 percent of enterprise desktops, highlights the urgent need for enterprises to improve the security and survivability of their personal computers. Many enterprises saw significant operational damage because of extended downtime caused by these attacks. Enterprises that had invested in strong desktop management capabilities and deployed centrally managed personal firewalls to every desktop did not see major damage from the Slammer, MSBlast and Sobig attacks of 2003. However, in the future, "day zero" attacks (attacks that occur before the software vendor has issued a patch) will increase. Thus, simply patching faster will never be good enough. By 2006, the percentage of attacks that occur before the majority of enterprises can successfully install patches will increase to 30 percent, from 15 percent in 2003 (0.7 probability).

Enterprises that maintain 10 percent or more of their desktops on an alternative operating system, such as Linux or Mac OS, are much less vulnerable to significant business outages than those that use only one operating system, such as Windows. By spreading critical business functions across multiple desktop platforms, or by maintaining key operating groups on separate platforms, you can enhance your ability to keep at least some of your key personnel and processes functioning and communicating during an attack.

The Security Benefits of Diversity
In nature, a forest that consists of only one type of tree is vulnerable to complete defoliation if an infection hits that tree species. However, if the forest has many varieties of trees, no single infection can cause catastrophic damage. Similarly, the adoption of a diverse operating-system environment offers three key benefits to enterprises:

- **Containment of malicious-code attacks.** The most-damaging virus and worm attacks target vulnerabilities in the Windows operating system. These blended threats leverage the continuing stream of Windows flaws to attack other Windows PCs and servers, causing catastrophic outages to enterprise IT systems. The use of alternative desktop operating systems by some critical personnel helps to prevent attacks from spreading enterprise-wide. These personnel can communicate and manage the network, and at least some core business processes can continue to function, greatly reducing the impact of an attack. *Enterprises that maintain 20 percent of their desktops on alternative platforms will see a 50 percent reduction in the scope of the business impact of worm attacks (0.6 probability).*

- **Competitive pressure on Microsoft.** Competition is always healthy for enterprise security because it leads to more pressure on vendors to meet enterprise security needs with innovation. If you make enterprise-wide security a key criterion in choosing operating systems, vendors will build more-secure products. If the impact of Windows security flaws enables Linux or Mac OS to achieve a small, but significant, portion of the desktop operating-system market — possibly at least 10 percent — Microsoft will be forced to respond by intensifying its efforts to make its platforms more secure. These efforts also will benefit enterprises because the vast majority of their desktops will remain on Windows.

- **Spread of technological innovation from one platform to another.** The Windows operating system is hindered by 15 years' worth of legacy code, which limits Microsoft's ability to make radical advances in security. As a key competitive strategy, Microsoft has continued to embed more functionality and application integration in the Windows operating system, greatly increasing its complexity — and complexity is one of the major enemies of security. Other operating systems do not carry this baggage; thus, they are in a better position to develop and deploy innovative security approaches. Microsoft will be able to use its strength in "embracing and extending" such innovation to speed the increase in security in the Windows platform. Enterprises benefit doubly when operating-system alternatives and Windows both improve in security.

**Diversity Is Not "Security Through Obscurity" — But Obscurity Helps**

Unix-based Web servers that run the Apache Web server have twice the Internet market share of Windows-based Web servers. However, the Windows-based Web servers have been successfully attacked at nearly twice the rate of the Unix-based servers because attackers are drawn to easy targets, and the endless stream of critical security vulnerabilities in Windows servers previously has made it "low-hanging fruit." Attackers will target gaping holes in non-Microsoft products as well, as the Slapper worm (which targeted Apache servers) shows. Moving to a combination of desktop operating systems mitigates the damaging effects of — but does not eliminate — cyberattacks.

However, moving all enterprise users off Windows is not the answer. Until an alternative operating system achieves 20 percent adoption in many enterprises, most attackers would not be motivated to develop worms or viruses because their "shock value" and the attendant publicity would be limited. Once it reached more than 20 percent adoption, the alternative desktop operating system would begin to see significant levels of attack. If it reached 30 percent adoption, it likely would see an attack rate almost equal to that for Windows. Of course, once an alternative operating system achieved this level of adoption, providers of firewall and antivirus technologies would be motivated to develop protective
products with new and innovative approaches. These innovations could be mirrored on Windows platforms.

Maintaining some corporate users on non-Windows desktops offers a huge advantage in terms of attack avoidance because the most popular target for virus and worm writers will always be the consumer desktop. If the corporate desktop is on a different platform from the consumer desktop, the majority of mass-attack worms will be avoided. Enterprises that stay away from products that are used by the consumer market will avoid attacks — just as trucking companies would not be adversely affected by a recall of flawed automobile tires.

**Diversity Has Significant Costs**

A diverse desktop environment is not the best choice for all enterprises. Diversity offers survivability from attacks, but it also generates numerous challenges for IS organizations. Gartner research has established that the total cost of ownership for heterogeneous computing environments is significantly higher than for single-system enterprises. Multiple operating systems inevitably require multiple IS skill sets for administration and management — the personnel with those skill sets will be more expensive.

The technical and organizational demands of administering multiple operating systems also present security problems. It may prove difficult — not merely expensive — for IS organizations to develop the necessary skills and management systems to administer more than one operating system at the desktop level. This skills deficit may result in implementation and management errors. Gartner research has shown that two-thirds of successful attacks take advantage of misconfigured systems. Tight administration of a single operating system provides more security than sloppy administration of multiple operating systems.

Enterprises that use significant numbers of fat-client applications that are tied to Windows desktop operating systems may find that alternative platforms are unfeasible. Enterprises that have no Unix- or Linux-based servers in place, or support no Macintosh desktops, may find that the costs of migrating to and maintaining a diverse environment are simply too high to even consider.

Enterprises that found that their desktop management and personal firewall strategies protected them from the impact of Slammer and MSBlast will find that the high costs of diversity are not needed for sufficient enterprise security. Enterprises that lock down desktops, have centrally managed personal firewalls installed on every PC and can push out critical patches to all desktops in less than two weeks after patch release will be safe from most attacks. However, attacks that happen before a patch is released will continue to be a threat. In addition, partially connected desktops are difficult to patch quickly, and to keep patched.

**A Simple Plan for Security**

Targeted adoption of a heterogeneous computing environment offers significant security value for some enterprises. Include the impact of recent worm attacks in your considerations of desktop operating-system choices. A simple way to begin this process is to move the elements of the IS organization that don't directly support Windows desktops and that don't require applications that are only supported on Windows onto an alternative operating system or systems. Thus, if a malicious-code attack strikes Windows, the desktops that run the alternative systems can function and can reduce the scope and duration of the attack.
Bottom Line: The adoption of a heterogeneous computing environment that focuses on specific business functions or groups can deliver valuable security benefits. Although this approach comes with significant migration costs and increased total cost of ownership, it should be considered by enterprises that were significantly affected by the SQL Slammer and MSBlaster worms.