Could Microsoft Make Security A Competitive Differentiator?

Date: August 29, 2005
Author: Jon Oltsik
Title: Security Analyst

Abstract: Have you looked at Microsoft's security efforts lately? If not, you should. The folks in Redmond have implemented some security best practices that trump much of the rest of the software industry. Don't look now but Microsoft could soon use security as a differentiator against 'asleep at the wheel' competitors.

As far as security is concerned, 2001 was a tough year in Redmond, Washington. With the U.S. reeling from the 9/11 terrorist attacks and security on everyone's mind, Microsoft was getting hammered. In September, while the company was still recovering from the August 'Code Red' worm, Nimda, a memory-only worm affecting Microsoft applications, spread like wild fire within a week of 9/11, flooded the Internet with traffic, and slowed response time down to a crawl.

Suddenly, Microsoft faced a series of unprecedented questions. Was Redmond doing enough to protect its customers? Did Microsoft's software dominance impact national security? Would we be safer if we migrated to Macintosh or Linux systems?

2002: Bill's Response

The devastating 2001 attacks were extremely painful to Microsoft. What's more, the Redmond management team looked at the world and realized that it was sitting squarely behind the eight ball as security would continue to become more and more important. Why? Because:

- **Large organizations were moving more traffic over public networks.** Big organizations across the globe were abandoning private network services like Frame Relay and ATM in favor of Internet-based VPNs. In addition, applications were becoming more distributed and communicating via middleware bridges over the Net. More exposure to the public Internet equals greater security risks – it's as simple as that.

- **Microsoft was THE target.** Microsoft was already the favorite object of teenaged hackers and script kiddies. Early attacks were annoying but global events like Code Red and Nimda demonstrated a real vulnerability associated with Microsoft's global reach. Customers were already screaming at Microsoft to improve security and the company had to be worried about massive liability litigation or government poking and prodding.

- **The future was at stake.** All of a sudden, competitors had a critical issue to throw in Microsoft's face. Linux seemed like a safer alternative, threatening future Windows penetration. In addition, without added security, bet-the-business initiatives like .NET and web services were as good as dead.

Far be it from Microsoft to wallow in self pity or sit on the sidelines. In January 2002, Bill Gates sent a memo to all Microsoft employees, issuing a security decree. Amongst other things, Gates wrote:

> There are many changes Microsoft needs to make as a company to ensure and keep our customers' trust at every level - from the way we develop software, to our support efforts, to our operational and business practices. As software has become ever more complex, interdependent and interconnected, our reputation as a company has in turn become more vulnerable. Flaws in a single Microsoft product, service or policy not only affect the quality of our platform and services overall, but also our customers' view of us as a company.

Bill's security manifesto ushered in the Trustworthy Computing era at Microsoft – "a long-term effort to create and deliver secure, private, and reliable computing experiences for everyone." Henceforth, the company would bake security into every product and process in an effort to improve its code quality and public reputation.

Microsoft Has Come a Long Way

As one could expect, Bill Gate's memo and Trustworthy Computing initiative received a lot of attention in industry, business, and government circles. Many pundits were skeptical about this new direction, dismissing it as a mere public relations stunt. A security push at Microsoft was just too big of a reach, the technology equivalent of Fidel Castro suddenly embracing U.S. style capitalism. Common wisdom said it could not and would not happen.

Fast forward three years to August 2005. ESG recently met with a number of managers from Microsoft's security team. While industry jokes and Microsoft bashers haven't lost their edge, there is a pronounced difference in the way Microsoft treats security. As Bill Gates recommended, security is now integrated into Microsoft's software development and daily business operations.

First of all, Microsoft has introduced a number of proactive steps to prevent security problems in the first place. This is a wise decision as it is generally known that fixing a security issue in development is far more cost effective than doing so in the field. To promote security best practices during the development cycle, Microsoft introduced its Security Development Lifecycle (SDL) which includes:

- **Mandating security training on a yearly basis.** All MS developers must take an annual training course to either learn or bone up on secure software development. Microsoft has recently expanded its training from a single course to an additional number of classes on specific security topics like vulnerability recognition and hacker behavior. At present, coders aren't tested on their security knowledge, but Microsoft does measure developer performance based on the quality of their work (or lack thereof). Microsoft is also ensuring future knowledge transfer by rotating developers between the security and Longhorn development teams.

- **Introducing security testing into each development phase.** At each milestone in a Microsoft product development lifecycle, the security team performs a security review of the design and functionality to minimize the risk of opening security holes. Before any product ships, it must go through a final security review process and the security team has the authority to hold up product release if it believes that security issues remain.

- **Addressing the Black Hat community with both a carrot and a stick.** Microsoft's more draconian tactics, like suing spammers under the CAN-SPAM anti-spam legislation, get loads of attention, but the company has also done a good job of reaching out to the Black Hat community to promote a state of détente. For example, Microsoft sent around 80 people to the recent Black Hat Conference in Las Vegas and hosted a "get to know you" party during the event. The company also invites some Black Hatters back to the Redmond campus to banter with developers directly. Microsoft calls this its "Blue Hat" conference.

Microsoft is clearly doing a lot of upfront work to prevent security problems but it also recognizes that bad things can still happen to good code. As a result, it also bolstered its ability to react to inevitable code vulnerabilities by:

- **Making its update process as efficient and seamless as possible**. The Software Security Incidence Response Process (SSIRP) is built on a meticulous and repeating 11-week cycle. Ultimately, most security updates are distributed to customers on a predictable schedule, the second Tuesday of each month. The update engineering process includes vulnerability definition, variant analysis, an application architectural review (with the appropriate application development team), testing, and release. The security team that manages this process is composed of a whopping 900 people distributed around the globe.

- **Performing a number of synthetic and real-world tests.** Microsoft security managers recognize that one of the worst things they can do is replace bad code with more bad code. To alleviate this risk, the team does rigorous testing on all update code. The routine includes a daunting combination of automated tests that throw a variety of attacks at application interfaces and live tests on Microsoft and selected customer networks.

- **Preparing for the worst case.** The recent Zotob worm activities illustrate this process. On Tuesday, August 9, the Microsoft Security Response Center (MSRC) put out a critical update for a plug-and-play vulnerability. Microsoft determined that hackers might subsequently exploit this hole, so it prepared accordingly, by developing user instructions, press responses, and a system clean-up executable if anything actually happened. Sure enough, the Zotob worm, a buffer overflow attack on the plug-and-play vulnerability, reared its ugly head on Sunday, August 14. Since the Microsoft team, through its Security Incident Response Process (SSIRP), had anticipated this attack, it was able to quickly respond with countermeasures, code fixes, and bulletins to help users minimize the impact.

- **Targeting Updates.** Microsoft reports that as many as 250 million downloads occur soon after it posts a new monthly update. Given the volume of downloads, even an extremely small number of bugs causes a big problem for the Redmond team. Microsoft has learned that the number of fixes (including customer hot fixes) included in a package directly correlates to overall update quality. To reduce the number of fixes that users receive, Microsoft has implemented what it calls a ‘dual tree’ process. This means that customers who have not installed a hotfix (i.e. the vast majority) get the security updates only. For customers who have installed hotfixes get all of the new security fixes without wiping out the hotfixes they have already applied. This works at the binary (DLL) level so every user is likely to receive fewer fixes than in the past, thus improving overall system stability.

Throughout the entire update cycle, Microsoft is absolutely manic about these processes – code simply can’t get out the door until every little detail is completed.

Could Microsoft Use Security As A Differentiator?

Its sounds like a stretch but technology vendor graveyards are filled with companies that discounted Microsoft’s ability to compete in areas like e-mail, database, and file-and-print. In the next few years, Microsoft could use its developing security prowess to outdo competitors in several ways, by:

- **Teaching Windows developers how to fish.** As Microsoft gets its own secure development process in order, it can bring that methodology to the armies of programmers who write code using Windows development tools. This could help the company beat others to market and claim the security high ground.

- **Applying its security principles to strategic new areas.** Microsoft is constantly expanding its footprint in markets like storage management, consumer electronics, and packaged applications. What if Microsoft trumped status quo vendors through security? Clearly this would be attractive in highly regulated industries and the public sector.

- **Develop a ‘trusted Windows’ environment.** Microsoft could harden some configurations and strip out unnecessary services to introduce a ‘Trusted Windows’ computing platform. Given its scope, this initiative would include security up and down the stack, from encrypting all file systems and databases, to making SSL the default for all network traffic, authenticating middleware messages, and including advanced access control/user authentication. Even IBM would have trouble responding to this type of coverage.

Bottom Line

Microsoft has proven time and time again that its corporate focus equates with execution excellence somewhere down the line. The company is now delivering on security in a way that sets it apart from other software companies. Yes, Redmond has a way to go to be considered a security company, but ESG believes that its security efforts should be taken seriously by competitors – and embraced by customers.