Security woes: Who is to blame? - Tech News - CNET.com

Newsmakers

Security woes: Who is to blame?

By Robert Lemos
Special to CNET News.com
November 8, 2001, 12:00 p.m. PT

newsmakers As the man who has to defend Microsoft's stance on Internet security, Scott Culp has his work cut out for him.

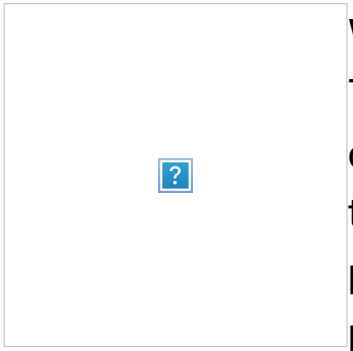
However, Microsoft--for so long on the defensive against hackers and online vandals--has decided to become more aggressive about getting its message out. And that has put Culp, the software giant's manager for security response, on the front lines.

In a recent essay posted on Microsoft's security site, for example, Culp, decried what he called "information anarchy"--the practice of not only finding flaws in software, but also of publishing methods of taking advantage of those flaws.

The issue is not new, but Culp's article marked the beginning of a push by Microsoft to call the security industry and hackers into account for distributing dangerous code. In many ways it isn't surprising, since Microsoft loses face every time a widespread security incident compromises its software.

However, if new vulnerability disclosure policies become widespread and cut down on the number of worms and attacks targeted at Internet companies, everyone stands to gain. CNET News.com caught up with Culp and quizzed him on Microsoft's new push for limited vulnerability disclosure and what the high-tech industry has to do to better secure its systems and networks.

Q: Why the name information anarchy?
A: Well, because it's accurate. The practice that the essay was discussing was the practice of throwing exploit information out freely on the Internet without regard to how it might be used. There has been a long debate, for years, about how much information ought be disclosed about security vulnerabilities. And for the longest time, folks arguing both pro and con could cite theory about why their position was correct. But the five worms (Ramen, 1i0n, Sadmind, Code Red and Nimda) that were released over the past year answer the question with actual data and conclusively.



What does that tell you?
Those five worms tell us the posting exploit information on the Web is harmful and dangerous. In all five cases, the worms were built using information that was publicly posted on the Web and posted to no good purpose.

Are you trying to hush up those that find these vulnerabilities?
Absolutely not. Our reputation and our practices speak for themselves. Nobody else in the industry is as open about reporting their own security vulnerabilities in their own products as Microsoft is. That's not going to change. And that is not what the essay is calling for. The essay is not calling for people to refrain from looking for security vulnerabilities, to stop reporting them to the vendors, to stop telling customers about them. We don't want to change any of that.
The only thing that we are suggesting is that reasonable people should be

able to agree that telling bad guys how to use those vulnerabilities to attack innocent users is wrong.

As far as releasing information and vulnerabilities, what about reports that the latest Windows XP patch has five security fixes, but only two are documented?

It's interesting that you can claim that you can know and don't know how many vulnerabilities are being fixed in the patch while at the same time saying you know how many fixes are in the patch. That seems to be a logical contradiction.

But let's talk about that update. It's the first critical update for Windows XP and contains all the fixes to Windows XP between the release to manufacturing and its availability in the market on 25 October. The idea between doing a single fix is that it is more convenient for customers because you only have to apply the one fix and you get everything. It can be applied at install time.

So when are you going to let users know what's in the fix on the security side?

The documentation that was released with the bundle discusses fixes that are not related to security and the documentation also discussed one vulnerability with Internet Explorer 6. And we released a vulnerability advisory last week that discusses a denial of service vulnerability. There is at least one other vulnerability that is corrected by that update for which a bulletin has not been yet released. And the reason is that we are completing the patches for other products that are affected by that vulnerability.

If we were to release information on that vulnerability at this point, it would put users of that other system at risk. But the minute we release the bulletin, we will tell customers what the fix is. What we are not going to do is make the information public when patches are not available for other affected systems, because that would put people at risk. This is

consistent with what we are describing in the essay.

How much of a difference will your new initiative make to Internet security? Are we going to see a big decrease in the number of worms?

We have to be realistic. There will be malicious users who will write malicious code. They will probably write worms, and they will attack users. The number of incidents will almost certainly be smaller than the number of incidents we have today. Judging by those five worms that tore through the Internet over the past year, recognizing that all of them relied on information that was posted to the Internet, we believe that denying malicious users that information can only help things. But we are realistic. We know it's not a panacea. We know that it won't solve the problems overnight, but it would raise the bar, and it would help the cause of security for our users.

Are you going for a mutual consensus of people here? What happens when a hacker finds a hole in some software package and posts it to a bulletin board or Usenet list? Is there anything you can do about that?

Microsoft is not the world's policeman. There is only so much that Microsoft can do. And the extent of what we are advocating now is self-restraint. We are not advocating the creation of cybercrime laws to prevent the posting of exploit code; we are not for any kind of punitive or coercive measures. We believe that security professionals, for the most part, are in this business to protect users--and that when they understand that certain actions are really protecting users, they'll do the right thing. So our goal here is, working with the rest of the industry, to try to develop some reasonable and moderate standards for handling security vulnerabilities that are likely to have the desired effect--that is protecting users.

It's been a bad summer for security. Code Red, Nimda, a Passport

vulnerability. There are those who might think this initiative is all about limiting the bad press that Microsoft has gotten in the wake of these attacks.

That's not true. There are a lot of dimensions to the problem of improving security. One of them is that vendors need to write better software, and we certainly count ourselves in that circle. We need to develop more secure products; we need to make it easier for people to manage their security on their machines. And we have been very up-front about our obligation to do that and our intention to do that.

For instance, the Strategic Technology Protection Program that we rolled out a few weeks ago. For the most part, it's a listing of the specific things we are going to change in our products to make them more secure. We have talked in the past about the secure Windows initiative and the steps we are taking at Microsoft to change our development practices so we can produce more secure software. We are absolutely committed to improving our products and realize that's an important dimension of the problem. But the handling of security vulnerabilities is another important dimension of the problem. We want to talk about all the dimensions at once.

Along those lines, what are we going to see in the future. Vulnerability disclosure has been an issue for a long time and most likely will continue to be an issue in the future. Are we going to see new initiatives from Microsoft to secure products?

The essay was intended to jump-start the debate in the community. We don't have all the answers. We are looking to other industry leaders to help us figure out what the next step needs to be. The essay was a problem statement--it identified a problem that needs to be solved. It wasn't intended to propose a solution; It was intended to start a debate about the problem. That's what we are here at the Trusted Computing Conference to do. We hope at the end of the conference we have some recommendations that we and the rest of the industry can make. You are

right that this is an issue that has been talked about for years. Our perspective is that it is time to stop talking. We all understand what the problem is. Now it is time as an industry to come up with a plan of what we are going to do to solve the problem and then start executing on the plan. ■

		Send us news tips