VOLUME THREE · ISSUE TWO
Secure Business Quarterly:
Defining the Value of Strategic Security

SBQ

SECURE BUSINESS QUARTERLY

SECOND QUARTER 2003
Exclusively on the Web at:
www.sbq.com

ILLUSTRATION: JUD GUITTEAU

Patch Management

Can't live with it, can't live without it.

Quantifying Patch Management

By Adam Shostack, CTO and founder of Informed Security

Secure Business Quarterly℠ is an @stake® publication.

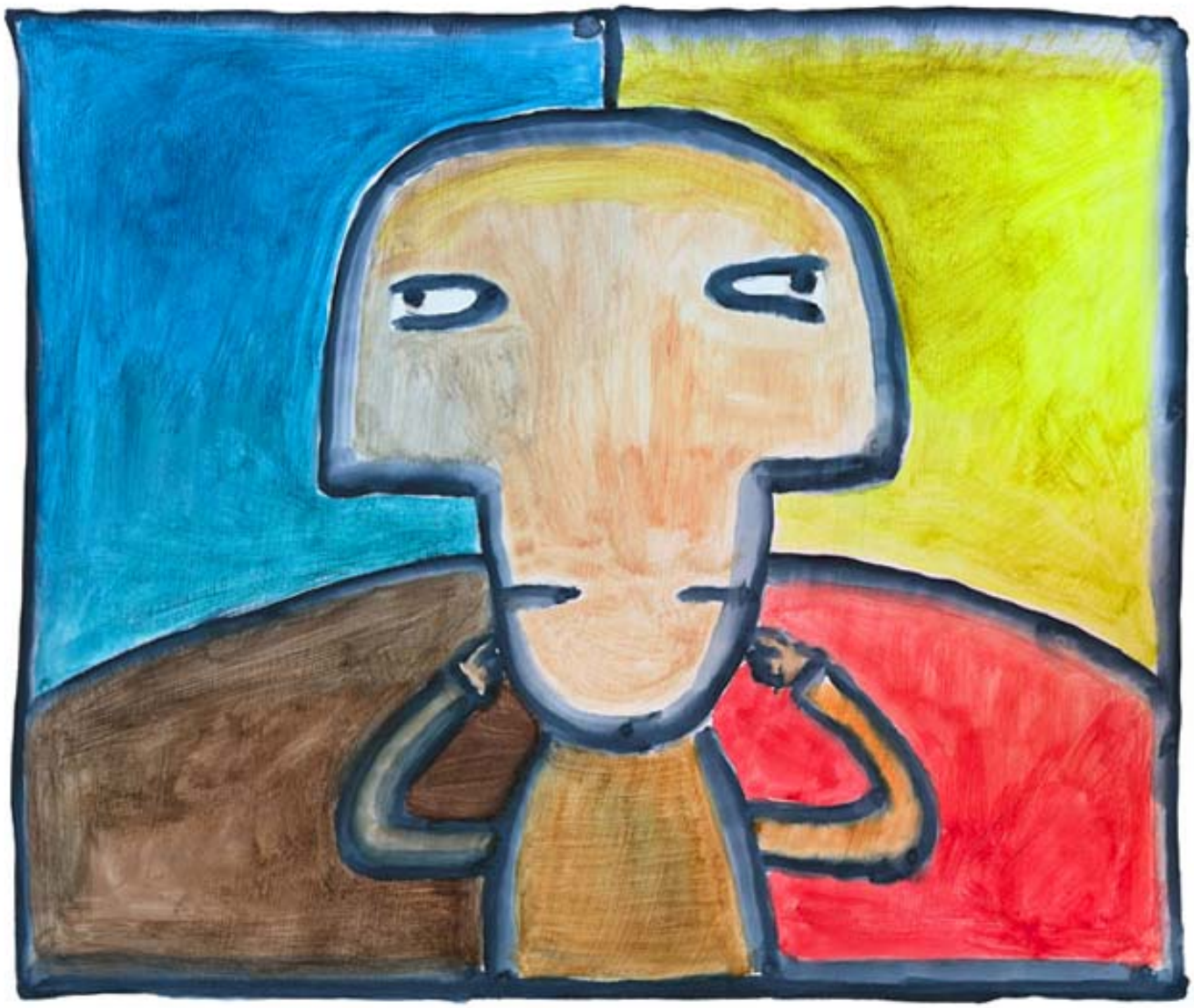

ILLUSTRATION: FRANK RENLIE

Quantifying Patch Management

By Adam Shostack, CTO and founder of Informed Security

Nine out of ten break-ins reported to CERT, the Computer Emergency Response Team, exploit known vulnerabilities. The most effective way to dramatically reduce the number of security incidents is to close the vulnerabilities that can be exploited without skill – in bulk or by a worm. However, vulnerabilities are left unpatched, sometimes for months and even years because of operational risks. Since the reality is that most break-ins take advantage of well-known problems where patches have not been applied, the question is obvious: how do we solve this problem?

Security experts often rely on vulnerability scanning tools to discover, catalog, and aid in the management of vulnerabilities. While these tools have their advantages, they also have a number of problems, such as that they slow the networks which they analyze; the inaccuracy of their results often requires further, in-depth investigation; and they generate a voluminous output of problems (and not solutions). These characteristics all stem from the fact that these tools are designed for use by security teams that need to find problems, not operations teams that need to implement solutions.

ILLUSTRATION: FRANK RENLIE

Security and operations are both actually right, but they are right at different times.

The operations/security divide also leads to trouble because the two groups see the world differently. To systems administrators, patches are risky, since applying them can break systems. Systems administrators are rarely rewarded for patches being installed, since successfully installing a patch means that nothing happens – apparently. This nothing, while good, *is* hard to notice, and is in stark contrast to a system being broken because of a patch. Security administrators, on the other hand, see *not* patching as risky. To them, the world is a vulnerable place, patches make things better, and the small risk of a patch being bad is a price worth paying.

Security and operations are both actually right, but they are right at different times. When a patch comes out, it is risky. Software has bugs when it ships, and even a small patch is software that is shipping for the first time. However, as users gain experience with the patch, they will discover if it has bugs and, if it is buggy enough, they will complain to the vendor, and it may even be replaced. This is why the risk of a patch causing problems declines with time; as the risk declines, so do the system administrator's concerns. (There is also a belief, grounded in experience, that not applying security patches doesn't lead to break-ins. People are bad at evaluating and managing low-probability risks.) Many administrators know this and use rules of thumb, such as "wait a week before patching." Security administrators, in turn, become more accurate as time goes on. (On the other side of the fence, code is written to exploit the vulnerability, and share that code within a small or large group. That code is debugged, and added to vulnerability scanners, worms, and other attack vectors. As time goes by, the rates of exploitation of a vulnerability rise.)

For security administrators, with each vulnerability, there is the need to protect against an ever-increasing possibility of exploits; simultaneously, for system administrators, with each patch, there is the need to delay its application in light of ever-increasing patch robustness. Closing vulnerabilities requires addressing both sets of concerns. This is possible by understanding that both groups perceive pressures differently but have the common goals of keeping costs down and ensuring ongoing operations. On a more practical level, since both risks change with time – one rising and one falling – there is likely to be a point where the risks balance. That time can be calculated.

Calculating the time at which the risks balance is a useful exercise, but it is even more useful to integrate business analysis into the calculation, and then to provide a value at risk calculation that can be used to drive patching decisions.

To calculate the value at risk, we need to know the expected costs of patching and not patching. Expected cost can be derived from a probability of a problem happening and the cost if it does

Imperfect risk measurements are better than no risk measurements.

happen. Further, all costs are relative to some business process that the computer in question supports. The failing system may be a desktop, a server, a router, a check printer, or anything else. The probability of patch failure can be estimated from a statistical analysis of how often the vendor's patches have failed in the past, and by examining which correlates of those failures are visible in a new patch. These odds can be calculated across all patches, across patches from a vendor, or even across patches for a given product if there are enough patches from that product group to make accurate calculations possible. Similarly, it's possible to derive the probability of a security breach for a given vulnerability; comparing the exploit rate of that vulnerability against other exploits can help provide this data. This information is being gathered by many vendors, including Symantec and Counterpane, and is also incorporated into measures such as CERT vulnerability metrics.

Beyond calculating direct costs, there are business-related risk measures. Is it the last week of a quarter? Is IT rolling out a new project? Is development rolling out a new product? These issues contribute to each decision of an IT department about when to patch or not to patch. System administrators need to move past the "every day is critical" approach and make a decision that acknowledges that the system is more valuable at some times than others. Ultimately, advanced risk management systems for patching will understand the business. (By the way, systems like phone switches that really do have requirements for 5 or 6 nines of reliability – 99.99+% – are engineered in support of those requirements. Other systems that need to function perfectly, from air traffic control to trading systems, have downtime built into their days.)

Though the ability to measure the risk of a patch is imperfect, imperfect risk measurements are better than no risk measurements. The current state of the world, where script kiddies can use known vulnerabilities to break into systems, demands better solutions than those deployed today.

Decision support for patch management thus needs to have a risk management system at its heart. Systems will be centered around risk management, because this is what makes it useful to a business. It will also need to integrate inventory management, patch deployment, and workflow management, but without risk management at its heart, the tool will not be useful – or used.

In short, since we can calculate the risks associated with closing or accepting a vulnerability, we can pay proper attention to the risks and choose the best time to address each one. SBQ

Adam Shostack is CTO and founder of Informed Security, the first company to deliver risk management for patches. He can be reached at adam@informedsecurity.com