one brightly cyber

WE MAKE CYBER SIMPLE

TO PATCH OR NOT TO PATCH

Limited cybersecurity budgets and staff mean enterprises have to prioritize where to spend scarce resources. With all the cyber risks, mitigation may be the chosen approach to many risks. This is understandable. If you consider the chances of the risk occurring remote, then mitigation may be the best answer.

Patching is a key cybersecurity task and can take significant amounts of time and budget. To offset this impact, some patches may be relegated to the mitigation category. After all, patching takes time and resources to test against all applications and operating environments and then promote to production.

This is time that can't be used for developing and testing new applications or features. While the patch is being promoted the website or service may be down. All these will impact the ability to bring in money.

Bringing money in is essential to the continuation of any business. But then so is keeping your website up, being able to serve customers, process orders and invoices, etc. That's where the balance between patching and mitigation can be tricky. You may feel the chances of a specific vulnerability being exploited on your systems are slim. They may be.

Allocating resources and funds is a management decision on where they will have the most positive impact for the company. It is always a guess, an educated guess, but a guess none the less. Looking at the probability of something happening is one side of risk management. The other side of risk management is determining what happens if the exploit is successful, the impact on the business.

In the case of patching, the impact of not patching can be minor or it can be major, possibly even catastrophic.

The recent Rackspace ransomware incident is a good example. Rackspace chose mitigation over installing a specific patch. The patch they didn't install resulted in a successful ransomware attack that took down their host Microsoft Exchange service.

Oops, not a good case for mitigation over patching.

To make the patch or mitigate decision more confusing, research has shown the score given to a particular vulnerability called the CVSS, Common Vulnerability Severity Scale, may differ between the national one from NIST and the one from the vendor.

Neither one is more accurate in all cases. We recommend looking at both scores and then looking at your environment to determine the risk, including the chances of it occurring and the business impact if it does.

For your evaluation take a look at the vulnerability and the possible risks it may impose. Has the vulnerability already been exploited? Is it actively being exploited by cybercriminals? Is the vulnerability being used for ransomware or an APT, Advanced Persistent Threat, that is one that stays in your system for a long time?

WE MAKE CYBER SIMPLE

TO PATCH OR NOT TO PATCH

Don't forget that a compromise of a low risk device may provide cybercriminals with access to more important devices. Or a way to contact people in the company from inside the company for business email compromises.

Be sure to evaluate all the risks of something occurring and the impact on your business before deciding on a mitigation strategy.

Let us reduce your stress.

Are you ready to get serious about protecting your assets and your company? Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.