Kathleen Allardyce
Freelance B2B Writer
GettingItWriteInc.com

PORTFOLIO: SYSTEMS ATTRACTING DATA BREACHES

Are Your Systems Attracting a Data Breach?

Are you doing everything you can to avoid a data breach? Most businesses are doing the best they can. However, there are forces working against you. Attracting and retaining cybersecurity experts is difficult, even if you have the budget for increased staffing. Besides that, a majority of breaches are a result of unpatched vulnerabilities, which means businesses need to make upgrades and patches a much higher priority than in the past.

Why Upgrading and Patching is so Critical

Upgrades and patches are a necessary part of keeping your systems running smoothly. Keeping track of the patches and getting them done is the problem.

When vendors discover a security vulnerability, the race starts. The question is, "Can the hackers get organized fast enough to hit the vulnerabilities before you can get the patches in place?" Too often, the answer is yes.

Upgrades, Patches and Data Breaches

Everyone is familiar with the Equifax breach. What many don't know is that unpatched vulnerabilities gave hackers the access to steal personal information, and cause a major systems and public relations disaster.

A study by ServiceNow and Ponemon Institute surveyed 3,000 companies to take a closer look at the circumstances surrounding data breaches. The study revealed that:

- almost half of the companies surveyed had a data breach in a two-year period
- 60 percent of the breaches were due to unpatched vulnerabilities
- 34 percent of the respondents who had a data breach knew that they had those vulnerabilities before the attacks occurred

Participants in the survey knew they needed to take action. In fact, 64 percent of them planned to fix the problem by hiring additional staff dedicated to updates and patches. This additional hiring would increase headcount by 50 percent for half of the businesses using this approach.

Kathleen Allardyce
Freelance B2B Writer
GettingItWriteInc.com

Is Increasing Staff the Answer?

Increasing staff is expensive. And, according to ServiceNow, it doesn't necessarily solve the problem. They believe that the shortage of cybersecurity experts is one major obstacle. They cite studies indicating that by 2019, the shortage of trained cybersecurity professionals will reach 2 million.

Therefore, even those companies who want to increase staff may not have the opportunity. Restructuring the patching process is a key part of fixing the problem. Results from the ServiceNow study shows that security teams spend an average of 12 days to coordinate patching systems across teams manually.

This is another classic business management problem where throwing people at the problem isn't going to fix it. There are just too many vulnerabilities and not enough people to find and fix them.

Where to Go From Here?

It's critical for every business to make the upgrade and patching problem more manageable. Here are some approaches to consider.

- **Address critical patches first.** Prioritizing patches is a critical first step. The first priority should be patches for vulnerabilities that hackers have found. The hacker world is a small community. Hackers quickly know which vulnerabilities their associates have successfully breached, and they will use that hack themselves.
- **Stress control.** Make sure that the privileges for different groups of users are well controlled. In addition, look for anomalous behavior that can lead you to spot an attempt to breach your system. Once hackers gain access, it usually takes some time before they're able to access sensitive data. Stop them while they're still researching your systems.
- **Look for outside assistance.** Rather than hiring additional staff, consider utilizing the skills of service providers who are already experts in implementing and maintaining mission critical systems such as SharePoint.

Client specific information removed.