one brightly cyber

UNIMPLEMENTED PATCHES DON'T HELP

The Log4j issue surfaced a few months ago. It is a serious vulnerability affecting countless computers.

The challenge this presented is that Log4j is not a bug, it is a feature intentionally designed into the Java programming environment. Log4j as its name implies is logging code for Java, a widely used programming language. The intent of Log4j is to provide a way for programmers to place certain result codes into a log that can be queried later by that program or by other programs.

Log4j is used by innumerable applications. The vulnerability allowed code to be executed remotely by cybercriminals. Being a specific capability built into the code and relied upon by an inestimable number of programs, it was more challenging to fix.

But, the severity of the problem had vendors scrambling to create fixes. They did create a fix and release it.

But that is only the first step. The patches need to be applied and, in some cases, the version of Log4j in use by a company needs to be upgraded. Sadly, recent research found over 90,000 servers still using vulnerable versions of Log4j.

Too many companies, especially small companies with limited IT staffs often put off installing patches or upgrading software. The reason is simply lack of staff or lack of time to test, install, and rollout.

Failing to stay current on patches and software upgrades is asking for trouble. Patches are never issued without a cause, often a vulnerability being exploited already.

Software updates may introduce new features, but often contain bug fixes to close known vulnerabilities.

Yes, we understand that the IT department is stretched thin. But a successful cyberattack can put your entire company at risk. The average time to discover a penetration may vary by industry but 2-3 months or more is not uncommon.

If you cannot show proper protections were implemented, expect regulators to impose fines in addition to the high cost of remediating the compromise. Regulators are raising the fines to convince companies that compliance is not only required but cheaper than paying fines.

Don’t forget the reputational damage a breach can cause, especially when it comes out, and it will, that you hadn’t properly protected information.

Don’t put off installing patches and doing software upgrades. As difficult as it may be, it is far better than the alternatives.

To learn more and see why we say Cyber Made Simple, visit us at onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.