**How did we get here?**

It’s reasonable to ask how this situa­tion arose. For example, are developers increasingly turning to OSS platforms and libraries to solve their problems?

“Obviously the benefits are hard to ignore with open source software,” says Fearon. “With business driving rev­enue and the time pressures that are on development houses at the moment, with quicker lead times for development and the competitive nature of applica­tions these days, using open source is an absolute requirement. Obviously there are cost benefits associated with it and there’s also an opportunity for learning. Because these are open source applica­tions, we can review others’ work – it’s more open and there’s more room for improvement. Generally it just drives improvement across the board.”

Of all those, cost and fast delivery are arguably the biggest drivers and many software and development houses would be hard-pushed to survive without using open source. But while the coders them­selves almost certainly understand that the library packages they’re including in their source code, or the development frameworks in which they’re building the project, are open source (and poten­tially subject to licensing restrictions such as the GPL), does this awareness. extend up the management chain, especially once you get to the C level?

“Essentially, I think there’s a lack of education, the higher you go,” says Fearon. “Obviously the developers are well aware. However, the management team above the developers are really responsible for understanding and creat­ing the open source usage policies that are required. It’s one thing saying we are allowed, or we approve a particular open source library. You need to understand what burdens those libraries impose. For example, what is the approval chain for understanding which open source compo­nents are applicable to the software that you’re building? And obviously there’s a business aspect. Once we start using open source, we get faster turnaround times, especially as more businesses adopt agile methodologies and the continuous inte­gration process. Higher up, at the board level, I think there’s a lack of awareness of how much open source is actually required in order to deliver that continu­ous integration environment and the con­tinuous release schedule.”

**Extent of use**

So just how extensively is OSS used within businesses? And what kind of security risk does this represent?

Black Duck regularly undertakes audits of business applications, often as part of merger and acquisition activities. Companies need to make sure, as part of their due diligence, that any software they are taking on board as the result of a merger doesn’t bring with it an unac­ceptable level of risk or create licensing problems. The firms may themselves undertake static and dynamic testing of code but that rarely identifies the full range of potential problems.

In its ‘Open Source Security Analysis’ (OSSA) report for 2016, Black Duck reviewed 200 business applications.1 Some 95% of these contained OSS components of some kind. The average number of components in each applica­tion was 105, 67% of the applications had vulnerabilities in those open source components and 40% of those vulner­abilities were rated as ‘severe’. Perhaps most puzzling was the fact that the average age of the OSS vulnerabilities was 1,894 days. In other words, these are likely to be well-known flaws for which potential attackers have had plenty of time to develop exploits. Indeed, 10% of the applications were vulnerable to the infamous Heartbleed bug in the OpenSSL cryptographic library.

Exercises

**1.Read the parts of article and find the answer for questions below. Answer in full sentence.**

What are arguably the biggest drivers of OSS?

……………………………………………………………………

What does Black Duck do?

…………………………………………………………………….

How many business application does the company reviewed in 2016?

…………………………………………………………………….

What are the average age of the OSS vulnerabilieties?

……………………………………………………………………

What is missing from programmers according to Feron

……………………………………………………………………

**2.** **Fill the sentences with number or phrase**

a)The average number of components in each applica­tion was …..

b)10% of the applications were vulnerable to the infamous Heartbleed bug in the ……. cryptographic library.

c)“Essentially, I think there’s a ………………, the higher you go,” says Fearon.

d)Obviously there are cost benefits associated with it and there’s also an …………….