Availability is a Diversion and We are Falling for It

Lori MacVittie, 2018-01-08

In a perfectly balanced world, availability and security would be equal. Surely the users of applications are just as concerned over the security of their data as they are with having access to it.

As we're all too aware, this is not a perfectly balanced world. Users are just as likely–perhaps more–to delete an app and desert a brand, thanks to availability and performance issues as they will due to a breach of data.

Oh, they still raise a ruckus over a breach. But it generally costs the company dollars instead of dedicated users.

That dichotomy is reflected in the priorities reported to us by security professionals in F5 Labs' 2018 Application Protection Report. Amongst CISOs, the number one concern is not–as you might suspect based on their title–security. In previous CISO-focused research, "The Evolving Role of CISOs and their Importance to the Business," a majority of CISOs stated their number one concern is availability, and that preventing application downtime is the primary mission for their organizations.

That was reflected, too, in our forthcoming state of network automation report. When asked what metrics are used to measure success individually and on a team basis, "network uptime" topped the list for 59% of security practitioners with "application uptime" coming in a close second with nearly half (49%) of security respondents.

Wrapped up in the term availability is performance. Speed is considered a component of availability, and security is often thrown under the bus when it comes to detecting the attacks that produce results. Because the data inspection critical to detecting malicious code and data is expensive and introduces latency, its practice is often viewed as counterproductive.

The focus on availability is an asset to attackers. Aware of their targets prioritization on availability, the F5 Labs' report notes, "attackers are also timing DDoS attacks as diversions to cover data theft and fraud attacks being pulled off simultaneously while administrators are distracted." This technique, known as a "smokescreen" is nothing new. As we noted in 2017, organizations are increasingly being hit by volumetric DDoS attacks to hide attackers' true intentions.

And consumers are paying for it.

Availability as a Diversion

Increasingly attackers are using our focus on availability as a diversion. That's troubling, because attackers are stepping up their tactics, employing every tool in their toolbox to find a route through the networks, infrastructure, and applications to the treasure trove that lies beyond its gates: data. The thing is, attackers aren't just using users and systems that stand between them and their goal. Today, they also use the data itself.

In F5 Labs' Application Protection Report 2018, researchers analyzed breaches and attack data from a variety of sources. The results were not unsurprising, but they are unsettling.

In the first quarter of 2018, 70% of breach records analyzed pointed to web injection attacks as their root cause. That's unsurprising if you've been following along. Over the past decade, 23% of all breach records indicate the initial attack vector as being that of SQL Injection. It's so pervasive that it was listed as number one on the OWASP Top 10 in 2017.

In fact, nearly half (46%) of attacks against PHP-based web apps were injection-based. Security professionals should take note that PHP is everywhere. Builtwith.com, which tracks the technologies used to build the apps that make up the Internet, notes that 43% of the top million web sites are built with PHP. The US hosts nearly eighteen million such sites, with nearly half (47%) of the top ten-thousand using the language.

That is a large field from which attackers can—and do—choose targets. Of the more than 21,000 unique networks over which attacks were conducted according to the report, 58% targeted PHP-based sites.

Data is a Growing (and Profitable) Target

Lest you point the finger at the language used, it is important to note that F5 Labs' researchers also caution to keep an eye on deserialization attacks. Such attacks are not language-specific and focus on the data itself. From the report:

"Serialization occurs when apps convert their data into a format (usually binary) for transport, typically from server to web browser, from web browser to server, or machine to machine via APIs."

By embedding commands or tampering with parameters in the data stream, attacks often pass unfiltered right into the application. Application—or application components—that fail to filter or sanitize the data can fall prey to vulnerabilities, as was the case with Apache Struts. Deserialization attacks are considered enough of a threat that OWASP added it to its top 10 list last year. Given that 148 million Americans and 15.2 million UK citizens were affected by just such a vulnerability, deserialization attacks warrant greater attention than they receive thanks to its relatively small use in the wild.

What's telling about these two threats is that they follow a common theme—you can't trust the data, either. Whether it's modified intentionally or riding piggy-back on legitimate requests, attacks are increasingly hidden in the data stream.

But lest you focus too deeply on the app and its data, let's not ignore that the rest of the stack is just as vulnerable and likely to be the target of attack. The continued reliance on weak encryption such as retired SSL and TLS 1.0 is a source of frustration. These methods have been retired because they're rife with insecurities and make it easier for attacks to exploit in search of access.

As the report notes, "New, named TLS protocol vulnerabilities are released about twice a year. However, with the exception of Heartbleed, the majority of named TLS protocol vulnerabilities are academic and rarely used in an actual breach. One of the biggest involved Community Health Systems (CHS) in 2014. CHS lost nearly five million social security numbers when an attacker used the Heartbleed vulnerability."

Low threat, high risk. No one wants to be that rare case, but eventually, someone is.

Security and Availability Should Both Have Equal Seats at the Table

The reality is that we're entering an age where it isn't enough to trust no one. We have to dig deeper into the stack to seek out attacks designed to disable and dodge protections put in place to safeguard apps and data. We must look at application protection as a continuum that is constantly evaluating the state of the entire application stack—from network to infrastructure to services. That means valuing the safety of our data as much as we do the speed with which we deliver it.

We need to remember Security Rule Zero: Never trust user input. And we need to also remember that user input includes data. That means stepping up security to include inspecting inbound data and finding ways to offset potential impacts on performance and availability.

It means recognizing that availability is sometimes just a diversion, and that we can't afford to fall for it. Security deserves —and needs—a seat at the same table with availability and performance. A CISO’s priority should be security, not availability.

Because if the CISO isn't going to go to bat on behalf of security, who is?

You can find more insights and analysis in F5 Labs' 2018 Application Protection Report, including helpful guidance on the attacks and protections that exist across the entire application stack.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | wwww.f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com