Addressing Evolving Application Threats

Raymond Pompon, Director of F5 Labs, discusses the complexities of protecting componentized applications and digital services and suggests ways to stay ahead of today's application threats.

How has application threat management become more challenging?

In the past, an organization would write a monolithic app, and a small group of programmers would write code and tie it to a database. Now, with the shift to more componentized applications, multiple libraries and tiers may be added, different teams — with different approaches — will work on different components, and it's all glued together with APIs. All these moving parts create more insertion points for an attack and more things that can fail in unexpected ways. In addition, with the dispersal of apps across the organization, it's much more difficult to fully understand and control an application's security and operations.

What gaps exist between perceptions of application security and actual security?

There are a number. People assume if they've outsourced something, security is included. That's not always true. On the development side, organizations may put together a series of components that are secure and stable on their own, but when assembled into an app, they create new vulnerabilities. Also, different components may have varying levels of security, and the weakest link in the chain creates an opening for attack.

How have digital citizen services increased risk?

With the growth in digital services, many organizations are using the same sets of apps and libraries across the entire organization. Different departments use them in different ways, but they all tie together because they use the same user ID for log in. The user can use this login ID to access all the organization's digital services. While that's convenient for the user and seems secure, what happens if a bad actor compromises the ID on a lower-value service with weaker security requirements? Now that bad actor is in the system with a legitimate ID, and they can move sideways to potentially gain access to more valuable assets.

How can organizations ensure that only the right users access applications?

No matter who comes through the door, you have to verify everything about them and that verification must follow them through the system. Organizations can't just check a user's ID, give them a password and be done with it. It's a continuous process of authentication. When a user attempts to move from one part of a system to another — for example, if a person applies for unemployment insurance, but they logged in through a parking application — the organization may want to require additional authentication or scrutinize the user more deeply. Access is not all or nothing. There's a granular dial that you're turning up and down based on what a user is doing within the system.

What are adjuvants and how can they help cybersecurity teams be more effective?

In medicine, an adjuvant is a substance that enhances the effectiveness of the main drug. In cybersecurity, adjuvants are people outside the security organization — they might be power users or have a special interest in security — who help fill gaps, act as liaisons, provide additional perspective and more. For example, adjuvants can share their knowledge of the organization's culture and processes to bring new cybersecurity hires up to speed more quickly. They can help roll out new concepts and policies. They can act as security evangelists and provide first-level support to end users within their group. And of course, they're also your recruiting pipeline. You can eventually bring them into your group when it's time to grow.

How can organizations "make the most" of a security incident?

Whether a security incident turns out to be a near miss or an actual breach, it provides an opportunity to learn how controls are failing and to find ways to fix them. Turning incidents into opportunities requires organizations to move away from blame. Often, the process is at fault, not the user. So it's about asking, in a very neutral way, "How do we fix that problem so we can react more effectively the next time?" You can actually get a lot of support when you say, "This is what happened; we identified these processes that could be tighter; and we'd like to change them in this way." And it doesn't always mean having to spend money. Sometimes it's just doing additional training or tweaking a configuration somewhere.

Cloud-native SaaS solutions for enhanced application delivery, security, and insight.

Robust Security

Your applications are automatically protected from multiple attack vectors with dynamic security options.

Cost-effective

Consumption-based pricing allows you to only pay for what you use.

Simplicity and speed

Easily provision and configure services within a few clicks.

Intuitive Interfaces

Manage services in an intuitive user interface or automate everything with declarative APIs.

Real-time visibility and analytics

Track performance, usage and billing with detailed reports and visualization tools.

Experience and support

Delivering 99.9 service guarantees with premium 24x7 support from experts with over 20 years of experience.

Learn more at: www.f5.com/products/ways-to-deploy/cloud-services