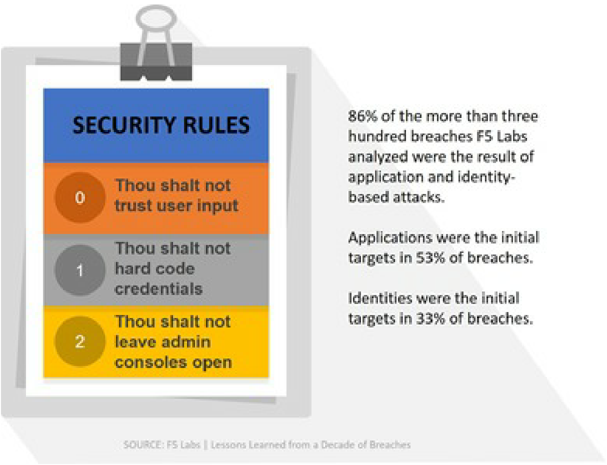
Containers, APIs, and Security Rule Two

Lori MacVittie, 2018-10-09

#LockTheDoor already


SECURITY RULES
0
Thou shalt not trust user input
1
Thou shalt not hard code credentials
2
Thou shalt not leave admin consoles open

86% of the more than three hundred breaches F5 Labs analyzed were the result of application and identity-based attacks.

Applications were the initial targets in 53% of breaches.

Identities were the initial targets in 33% of breaches.

SOURCE: F5 Labs | Lessons Learned from a Decade of Breaches

You would think by now that nothing about security would surprise me.

Maybe it's not that I'm surprised, but rather I'm disappointed.

Disappointed in the failure to adhere to even the most basic of security principles. You know, like lock the door.

A recent report from Lacework highlighted the need to reiterate one of the common core security rules:

THOU SHALT NOT LEAVE ADMIN CONSOLES OPEN

The report, which scanned the Internet, discovered "more than 21,000 container orchestration and API management systems" accessible.

That, in itself, is not concerning given that 95% of those were running in AWS. If you're going to deploy containers and API gateways in the public cloud, you need to be able to manage them. That's most frequently going to be accomplished via some sort of operational console.

What is concerning is that more than 300 of those dashboards were found to require absolutely no credentials to access.

I want to note that it isn't just the Lacework report that notes this existential risk. Back in May 2017, the RedLock Cloud Security Report published its finding of hundreds of Kubernetes administrative consoles accessible over the Internet without requiring credentials.

So this not a new thing, but it is a thing we need to try to get ahead of before widespread adoption ramps up further. Because one of the things attackers do with these open consoles is fire up their own containers to conduct a variety of nefarious activities such as bitcoin mining and bot execution. They aren't necessarily after your data, they want free compute and a fresh set of IP addresses that aren't currently blocked on blacklists across the Internet.

And they want the unfettered outbound access they all too often find in these environments. The most recent RedLock report found "85% of resources associated with security groups do not restrict outbound traffic at all. This reflects an increase from one year ago when that statistic was 80%." With no restriction on outbound traffic, it's no surprise the RedLock team also found about 39% of Amazon-deployed hosts it monitors "exhibiting activity patterns associated with instance compromise or reconnaissance by attackers."

It should go without saying that if you're running a web- or API-based console of any kind you need to lock it down. At a bare minimum you need to require credentials.

I know organizations have a zillion security rules and checklists that can seem overwhelming. But almost all of them can be generalized to fit these three core security rules:

1. Thou shalt not trust user input. Ever.

2. Thou shalt not hard code credentials. Ever.

3. Thou shalt not leave admin consoles open.

They're simple rules, but the simplest answer is usually the right answer. And right now, even the simplest security measures will yield a most positive security posture.

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