Poor security practices in the cloud

By Lori MacVittie

12 Apr 2019

So far this year, there have been five documented cases of organisations exposing their private data due to misconfigured S3 buckets or cloud databases.

Lori MacVittie, Principal Threat Evangelist, F5 Networks

Wait, let's fix that: due to intentionally configured S3 buckets and cloud databases. The distinction is important. In order to allow the kind of access necessary for unauthorised users to view S3 buckets or access databases, someone has to intentionally remove or degrade the default security guards placed on them.

To call them misconfigured implies a mistake, the kind that everyone makes from time to time and can be forgiven. But these are not mistakes. These resources have been intentionally opened up to allow access to just about anyone.

F5 Labs researchers combed through lists of organisations whose cloud resources have been exposed since 2017 due to intentional insecurity. The growth rate from 2017 to 2018 was an alarming 200%.

So far in 2019, with an average of 2.5 breaches per month, we would expect to see a total of 30 breaches by the end of 2019. Yet, the 2017-to-2018 growth rate tells us that our estimate for 2019 is probably far too low. If the 200% growth rate were to continue, we'd expect to see as many as 90 cloud security breaches in 2019.

What's worse is that we're sure that our compiled lists of organisations are only scraping at the top of the barrel.

This is not acceptable. Not only is private data exposed, but some of the data also has the potential for very real, very damaging repercussions for those to whom the data actually belongs. You. Me. The guy in the next cube. The woman getting off the bus. The teen readying for college.

Here are just a few breach examples:

- In 2017, a credit repair service exposed its customer's data. How long do you think it took for predatory scammers to find that and exploit those whose only crime was trusting a company to help them repair their lives?

- In 2018, a home security system used the same hard-coded keys on devices as it did for its AWS storage server, where recordings detailing home layouts were sent. How long do you think it took criminals to find and exploit the intimate details or occupancy patterns they were able to discover about customers' homes?

- Most recently, a data analytics company servicing financial organisations leaked 24 million US loan records via an exposed database with no password. No doubt predators, scammers, and identity thieves threw a party to celebrate.

No industry is left out of the growing list.

From governments to service providers, from manufacturing to politics, from finance to entertainment, every industry has an entry in the "Who Can Lose the Most Data Due to Poor Security Practices" contest. It's a contest no one should want to win - or even enter in the first place.

We are firmly entrenched in the digital economy. The bits and bytes that fuel it don't just represent dollars or yen or pounds. They represent people. People who are actually impacted by these breaches in ways we may never know because it doesn't get reported.

How and why is this happening?

Why would someone intentionally compromise their security when configuring S3 buckets and cloud databases, making them public-facing? In our experience, the culprits are rarely on the operations side: network engineers, database administrators, systems engineers, and security engineers would know better than to do this.

- Network engineers, typically responsible for managing access to systems over the network and determining which systems are public-facing, would not generally allow a database to be public-facing.

- Database administrators, typically responsible for managing database access and account permissions, would not allow databases to be accessed without requiring authentication. They would take on enterprise password policies with standard complexity requirements and not allow weak passwords.

- System engineers, typically responsible for managing applications to the defined hardening standards, would manage a web server in front of the public-facing database and would ensure it was properly secured with a web application firewall.

- Security engineers would normally conduct independent assessments of all systems and the network to ensure

compliance with the security policy.

More often, the product development side might decide not to incorporate already-existing security features - in many cases because they don’t want to disrupt the revenue stream, either by pushing back the timeline or potentially introducing new bugs.

Moving to the cloud enables developers to circumvent traditional enterprise IT roles that are obviously needed, considering the growing number of cloud breaches. That sets up the perfect storm for devs to deploy systems with poorly-configured security features, not because they want to, but because they might not understand the consequences or they might assume that a breach is unlikely to happen.

What you can do to avoid cloud breaches

How do we fix this problem? No one is suggesting we go back to long, extended delays in deploying systems (a common dev complaint). At the risk of doing time in Buzzword Jail for this, maybe as an industry, we should start talking about DevSecOps as a discipline to infuse good security practices into development.

All teams clearly need to be included in the conversation. Only limited security reporting is available in default cloud deployments: there are no trusted network engineering or systems engineering teams from which to request a list of subnets and ACLs, and no Active Directory groups and permissions. In most public clouds, organisations need to buy third-party cloud security auditing tools to produce the reports the security team would normally have gotten from their internal counterparts.

Yes, security is hard. Yes, security sometimes slows things down. But intentionally ignoring or degrading security because it's more convenient or speeds up the process is simply unacceptable and quite possibly unethical. Real people can be impacted, and not just financially. That's real people, not just the digital incarnations they entrust to companies on a daily basis.

It's time to stop referring to these exposures as the result of misconfiguration and start calling them what they are: intentional and deliberate insecurity. More importantly, InfoSec professionals need to call out these poor practices more firmly. Perhaps with a reminder that poor security practices impact people and not just the processes they're used to avoid or circumvent.

ABOUT THE AUTHOR

Lori MacVittie, Principal Threat Evangelist, F5 Networks