TAG CYBER

Case Study: Securing Access Entitlements in the Cloud

In this business case study, an executive team discovers some difficult truths about their cloud security posture when analyzing how another financial institution was breached and if they might be vulnerable to similar attacks. Learn how they dealt with the issue and use the discussion points to explore how your team may address similar problems.

Prepared by

Adam LeWinter
Senior Analyst
adam@tag-cyber.com

It was a breezy Thursday morning as Jim Harrison walked through the parking lot from his car to the beautiful red brick office building that housed Kurdon Financial headquarters. He adjusted his tie knot as he entered the atrium and checked his appearance one more time in the mirror hanging on the wall. His face showed the results of the sleepless night he had just had while preparing for this meeting. One of their competitor financial institutions, Tyden Bank, had suffered a very public and embarrassing breach inside their public cloud infrastructure the week prior, and the CEO of Kurdon had almost immediately scheduled the meeting to discuss their risk of a similar breach.

That was a hard question to answer, as the investigation into the breach was ongoing. As Chief Information Security Officer at Kurdon Financial, Jim shuddered as he thought about what it would be like if he had to deal with a breach that caused the theft of hundreds of thousands of customer accounts and personal information. The first technical analysis report had been released the night before, and Jim had forgone sleep to go over it with his security team. Jim and his team were determined to ensure nothing like what happened with Tyden Bank would happen at Kurdon Financial.

Like Tyden, Kurdon had been relying on public cloud providers to host their customer portals for years. Jim wanted a full review of their cloud security posture. A key takeaway from the technical analysis report of the Tyden breach was that the native security controls offered by the public cloud provider were not enough. His team was still analyzing the report, but it was time to discuss the initial findings with executive leadership.

The Executive Leadership Meeting

As Jim walked into the conference room, he saw Ben Swanson, Kurdon's CIO, already sitting at the table drinking a cup of coffee.

"Geez Jim, you look like we were the ones breached," Ben said as he sipped his coffee.

As Jim gave a dry chuckle and sat down at the table, Sarah Mullane, Kurdon's CEO for over a decade, walked into the room. "That's exactly what I'm looking to avoid," Sarah said, "and I hope you are ready to tell me why we won't be on the front page of the newspapers in the future just like Tyden."

"There is nothing to worry about," said Ben, as everyone found their seats and the meeting officially began. "Our cloud automation and quality controls are much more mature than what Tyden had running. I spoke with the Tyden CIO, who is a friend of mine, and she said the entire thing was caused by a vulnerability in the firewall. We have a better cloud deployment strategy that is designed to prevent this exact scenario." Sarah turned to Jim, "Jim, do you agree with Ben that this is something we already have controls in place for?"

"Let me start by saying that the technical analysis report of what happened was just released last night, and I have my team analyzing it thoroughly to determine how our security posture compares. That said, Ben is correct that it appears the breach was caused by a vulnerability in the firewall. However, what concerns me is how the breach progressed once they found their initial entry point. I worry we might need to reconsider our public cloud security posture."

"Nonsense!" Ben interjected, "We have invested heavily in tools to ensure our cloud presence exceeds all compliance standards."

"This isn't just about compliance, Ben. The public cloud service providers have been proven to do a good enough job protecting their environments, but we are responsible for securing the data. There are steps we take to protect it as dictated by compliance, such as encryption and utilizing a web application firewall, but I'm willing to bet Tyden also met or exceeded all compliance standards and they were still breached."

"Right, because of a firewall vulnerability," Ben responded, "and, as I said, we invested in our continuous integration and deployment pipelines with tools to prevent this exact scenario."

"What has me concerned is the potential that one misstep with a firewall can open an avenue for the attacker to get access to our sensitive data," Jim continued, "I'm uncomfortable with the idea that the only thing between them and our data is reliance on correctly configured firewalls. We have a massive and complex cloud environment hosting many apps from different business units. I believe it's impossible to guarantee the firewall controls will always be flawless, despite the best intentions of our developers and their tools. We need to find a way to limit the blast radius if somehow they get a foot in the door."

"If you add more stringent controls on top of what we already have, developers will be constantly blocked when trying to do their jobs. We cannot slow down our development speed here," said Ben.

"Jim, you said your team was still investigating the report?" Sarah asked.

"Yes, we have a team meeting scheduled right after this to look at the finer details to see if we need to adjust our security posture."

"Excellent. I want you and your team to report on any risk that we might have and work with Ben on how we will mitigate it," Sarah said, "Kurdon must not make headlines because of a security breach as we look to continue our international expansion this year."

Jim nodded. He knew that any negative press would hold back Sarah's plans for further international expansion, and the personal reputational damage would certainly hold back his career advancement plans.

The Security Team Meeting

Jim walked into the conference room and was surprised to see papers strewn on the table and being scrutinized by many members of his team. He found Jennifer Minton, his security operations center (SOC) team leader, staring intently at a sheet of paper in her hand.

"I thought paper was a thing of the past," Jim remarked, bemused by the scene.

"The technical analysis of the Tyden breach is full of diagrams --I didn't have time to copy them into slides," Jennifer said as she placed the paper she was holding on the table. "Looking at them and reading through this has me concerned about our public cloud security posture."

"That's exactly what Sarah wants us to examine. What have you found?" Jim asked, addressing all in the room.

"Well, at the top level, the breach was caused by a vulnerability in the firewall. Once the firewall was compromised, the attacker had access to the machine and its credentials which were leveraged to further access the environment. The excessive access entitlements of the credentials allowed the attacker to use the machine as a proxy for further malicious activity in the environment," Jennifer explained.

"It's a good thing we spent all of last year implementing that cloud security posture management tool. Now that we are finally using it, we have a greatly reduced chance of vulnerabilities and misconfigurations," said Sam Hertz, a security engineer. Sam had spent almost 11 months working with Ben's team to implement a CSPM tool to clean up the simple audit report findings that constantly appeared.

"CSPM tools don't protect firewalls from vulnerabilities," Jennifer continued. "Besides, that was just the entry used by the attacker in this case. We could have a flawless firewall and still be vulnerable because once another attack avenue is found the same underlying problem exists."

"Seems to me that the underlying issue was whatever caused the flaw in the firewall," Sam persisted.

"You are focusing on the wrong part. A firewall vulnerability is simply one of many possible ways to gain entry to an environment. The more serious problem is what the attackers did once in. They stole the credentials assigned to the virtual machine hosting the firewall, which had excessive access entitlements, and used them to gain unfettered access to the entire environment. The credentials were valid so the attacker's actions weren't flagged as an issue," Jen explained.

"Clearly they just had their multifactor authentication and single-sign-on policies wrong. We've done a lot to protect our identity with big investments in MFA and SSO," Sam said.

"These credentials aren't protected by SSO or MFA because they are not user accounts. They are accounts used by their apps to validate identity internally. The bigger issue here is what entitlements the credentials had. With no check on what the credentials should have access to, it was easy for the attackers to use them to move throughout the environment," Jen said as she looked at Jim. "We have a similar issue. My team needs to be able to monitor and clearly understand what each credential set has access to."

"So you want a privileged access management solution? Do those even work in the cloud or in an environment as complex and dynamic as ours?" Sam asked. "We have so many different containerized environments with ephemeral hosts that the raw data alone would flood our SIEM and make it impossible to find anything."

"You're on the right track," Jen said. "PAM solutions work in data centers but are not designed for dynamic cloud environments. What we need is a similar solution for the cloud as well. We need to not just identify all human and machine identities, but also analyze their entitlements, roles, and policies. Our environments are dynamic, so we need to use a continuous lifecycle approach that allows us to follow the environment changes over time."

"That would mean the tool would need to be just as agile and automated as the rest of the environment," Sam said. "Do we even have the ability to build that?"

"Ultimately, this attack was the result of a vulnerability. Exploitation of the vulnerability made this entire scenario possible, but the subsequent lack of entitlement controls turned that vulnerability into a full compromise. Our environment is large, complex, and dynamic. Vulnerabilities are going to happen. What we need to ask ourselves is how we limit the impact," Jennifer said.

Jim looked around the room. He could see everyone nodding in agreement as they came to grasp the broader threat. "Thanks, Jennifer," he said. "Now let's figure out how we can address this without flooding our SIEM or needing to build an entire product, and in a way that Ben and his team can get on board with…"

Topics for Group Discussion

The access entitlement risks that Jim and his security team at Kurdon Financial came to understand they are exposed to are not unusual, even for a bank. While most enterprise security teams focus on preventing compromises, the complexity of cloud environments means vulnerabilities and misconfigurations are never going to be fully eliminated -- and software will always have new vulnerabilities. The move to cloud has spurred the use of automated tools in the development pipeline, with growing automation of most administrative tasks which use privileged service accounts. The entitlements of all identities should be a major area of focus for security teams, especially when dealing with machine identities, to avoid, mitigate, and allow investigation and remediation of related risks. A strategic approach to access entitlements also goes hand-in-hand with the recognized need for zero trust and least privilege security.

Some recommended topics for group discussion based on this case study are listed below:

1. *Risks* – How is your organization currently assessing and managing identity-related cyber risk?
    a. *What tools and processes are you using, and how often?*
    b. *Who is responsible for assessing risk related to your cloud identities and entitlements and how is that risk communicated through your organization?*
    c. *Are you comfortable with your current visibility into the identities with access to your cloud infrastructure and resources?*
    d. *How do you prioritize which access risks to monitor or address?*
    e. *How quickly and broadly can you make changes to permissions policies to mitigate risk?*

2. *Roles and service accounts* – Depending on the clouds in use the terminology may be different but, in general, trusted machine entities, or service accounts, take on roles that give access to resources. How many machine identities or service accounts do you have in your ecosystem? What services are they being used by?
    a. *How complex is management of these service accounts?*
    b. *Do you have granular visibility into all of the entitlements that each service is explicitly or implicitly granted?*
    c. *Are the service accounts limited to just the entitlements they need?*

3. *Tools* – Which commercial or open source tools are you aware of that might help reduce this risk to your access entitlements? How might these be identified, researched, and tested?
    a. *What types of tools are you using today to detect these types of problems?*
    b. *How does your organization improve its research and source tool selection in this area?*
    c. *If open source, what kinds of resources are you dedicating to your open source solution and what outcomes are you seeing?*
    d. *What are your top business requirements for access entitlements and how does each vendor align?*

4. *Plans* – If you were part of Jim's team at Kurdon Financial, what would your plan be for addressing the access entitlement risk that Jennifer identified?
    a. *How would you obtain buy-in and support from Ben, the CIO, and his team?*
    b. *What is the mix of people, process, and technology required for your plan?*
    c. *Estimate the time and cost requirements for such a remediation plan.*
    d. *How would you ensure the implemented process does not impede development velocity?*

5. *Compliance* – What are the main compliance considerations for your organization and industry with respect to your public cloud infrastructure/deployment?
    a. *How do access entitlements relate to your compliance regulations?*
    b. *Which regulations and laws are your organization subject to?*
    c. *How are you auditing compliance?*
    d. *What are the implications of a compliance failure?*