Case Study:

Fully Migrating a Telecom Company to the Cloud While Successfully Addressing a Security Breach Within Their On-Premise Infrastructure

COMPUQUIP
CYBERSECURITY

I. Introduction

Security breaches occur when an intruder gains unauthorized access to an organization's protected systems and data, an early-stage violation that can lead to things like system damage and data loss. In 2019 alone, there were just over 7,000 reported breaches, with more than 15 billion records exposed as a result. Cybercriminals use hacking techniques and malicious applications bypass security mechanisms to reach restricted areas.

> *In 2019 alone, there were just* **over 7,000 reported breaches***, with more than 15 billion records exposed as a result.*

These attacks cause damage to an organization's reputation and can occur on a massive scale. This case study will explain how Compuquip Cybersecurity successfully contained a data breach on a telecommunications company's on-premise environment AND successfully migrated their entire infrastructure to the cloud.

II. Project Background

The unique aspect of this case study is that not only was Compuquip Cybersecurity called in to analyze and contain a security breach, but we were also able to fully migrate the client's entire on-premises infrastructure to the cloud on the other side of the incident. This was a fixed fee project that was delivered on time and within budget.

III. The Breach

Given the urgency of the situation, our engineers were under intense pressure. Fortunately, the Compuquip Cybersecurity team has years of experience in how to approach security breaches. The initial threat was contained within 24 hours, and systems were recovered and restored to the cloud shortly afterward. Compuquip Cybersecurity also noticed that the telecommunications company didn’t have an effective incident response (IR) plan in place, which can be disastrous for any organization.

Knowing this, we worked with the client in the aftermath of the breach to assist them in developing an IR plan that included the following key steps:

- Preparation
- Identification
- Containment
- Eradication
- Recovery

IV. Cloud Migration

The cloud migration project consisted of transferring the critical on-premise servers first, which took about 24 hours to plan and execute. Additionally, we deleted all malicious artifacts from the ransomware and moved 7TB of data to the cloud for users to access within 24 hours as well, which was a huge accomplishment.

V. Business Benefit

The benefits of implementing an Incident Response Plan for this organization included:

- Being prepared to face security incidents confidently and effectively.
- Mitigating the potential damage after a security incident.
- Maintaining the trust relationship with customers, partners, and investors.
- Improving communication between different departments.
- Strengthening defenses against future incidents with lessons learned.

The benefits of migrating to the cloud for this organization included:

- Scalability
- Cost-Effectiveness
- Remote Collaboration
- Integration
- Disaster Recovery
- Task Automation
- Enhanced Flexibility and Agility
- Reduced Maintenance

Of all the benefits of moving to the cloud, this telecommunication company benefited the most when it came to reduced maintenance. Since the company didn’t have a strong security team to keep up with system patches, we believe that an unpatched vulnerability was the primary vector of attack.

Moving to the cloud allowed the client to focus more on its primary business while the cloud provider handled critical infrastructure issues like patching, updates, and access control.

Savings Impact

Cost savings is one of the main reasons why organizations migrate to the cloud. By moving to the cloud, this telecommunications company was able to lower its capital expenses since it no longer had to purchase or maintain hardware and equipment. These savings are quite significant since it not only includes the expense of the initial purchase, but also the cost of unused resources. With cloud-based services, customers only pay for the computing resources they utilize, avoiding the wasteful costs associated with server sprawl.

Translatability

Many of the areas found within this telecommunications company's on-premise environment were translatable to the cloud. The chosen cloud provider had many options to choose from when it came to selecting the instance most appropriate for each IT function. Migrating to the cloud does come with a number of new terms and those who are mainly familiar with on-premise environments might have to take some training to learn more about the cloud space. Compuquip Cybersecurity provided initial cloud training to familiarize the team at the telecommunication company.

VI. Lessons Learned

Cloud infrastructure is complex and should be planned out ahead of time. Since we had to act quickly after the breach, we decided to build an ad-hoc cloud environment without mapping the network topology beforehand. Although the incident and resulting downtime had a lot to do with this, this plan of action is not recommended in the future.

VII. Conclusion

Being able to tackle not only one huge task (the security breach), but also migrate an organization's entire infrastructure to the cloud in a short amount of time was a great win for both the telecommunications company and the Compuquip Cybersecurity team. Not only does Incident Response Planning prepare you to face security incidents with confidence, but it also helps your organization mitigate damage to your operations, strengthen relationships with your stakeholders, improve your interdepartmental communications, and make you stronger to face potential cyberattacks going forward.

Cloud computing is considered one of the cutting edge technologies of the 21st century. Its innovative ability to provide relatively inexpensive and convenient networking and processing resources has fueled wide-ranging adoption in the computing world. However, cybersecurity should always be a priority whether your infrastructure is located on-premises or within a public cloud platform.

COMPUQUIP
CYBERSECURITY

Email: info@compuquip.com

Phone: 789-641-5437

Address: 2121 Ponce De Leon Blvd. Suite 530
Coral Gables, FL 33134

Follow us on: