How to prevent the next attack?

Lessons from the Capital One Breach

1. What Happened ?

On July 29 Capital One Financial Corp., the fifth-largest U.S. credit-card issuer, disclosed that it was the victim of a breach that exposed more than 100 million consumer applications for credit https://www.capitalone.com/facts2019/. Paige Thompson, a former Amazon employee, was arrested in connection with the hack by federal agents and charged with accessing customer data that the bank had stored on Amazon's AWS cloud service. The Capitol One breach is one of the largest and most impactful cyber incidents in recent history. The US Congress has launched an investigation into Capital One and Amazon to probe the causes and consequences of this breach.

2. Exploited Security Vulnerabilities

In the case of Capital One there were three main areas of vulnerabilities that led to the breach:

1. Capital One had an internet facing web application deployed on AWS EC2 instances. The application was vulnerable to a Server Side Request Forgery (SSRF) attack. This type of attack allows the execution of remote commands which can enable access to non-public endpoints. The ModSecurity web application firewall (WAF) module that was deployed with the web server was not configured to block SSRF attacks.
2. The web server's AWS IAM role had broad permissions and AWS IAM S3 bucket policies were not restrictive enough. This allowed the attacker to remotely access customer data stored in S3 buckets by assuming the role of the web server.
3. Capital One did not perform effective vulnerability scanning and intrusion monitoring of web applications to detect SSRF attacks. Vulnerabilities of deployed IAM policies were not detected with automated compliance checking tools.

3. Lessons to be Learned

It is HolistiCyber's practice to systematically identify the vulnerabilities that hackers are exploiting and to analyze the kill chains that lead to successful compromise. Understanding how malicious actors operate is essential to set priorities for protecting critical assets and to focus on risks that matter most.

Some of the lessons of the Capital One incident include:

- There were seemingly no AWS vulnerabilities exploited in the attack. However, the AWS security model is very sophisticated and complex; it consists of many layers and components and each service requires its own security considerations. The shared responsibility model puts a heavy

burden on organizations who use the cloud. Designing, configuring, testing and monitoring the many complex security controls requires deep knowledge and expertise.

- The most important aspect of securing resources in AWS is managing identities, roles and access policies. If access controls to resources are enforced by adequately restricted roles and IAM policies then then the attacker's access is limited, regardless of how he or she initially penetrated the environment. IAM serves as an effective security control for many different attack vectors, including some attacks from the inside. Implementing complex, fine-grained IAM policies can be a non-trivial task, however.
- Architectural security principles such as defense in depth and least privilege should be incorporated into every application design. Using multiple independent security controls and tightly restricted roles will prevent unauthorized data access.
- Encryption: AWS managed server-side encryption can generate a false sense of security. In the case of the Capital One attack transparently managed encryption would not have prevented the compromise of the stored customer data. Encryption with customer managed keys (CMK) with separate, individual key policies or client-side encryption can provide better protection.
- Even though the accused attacker was not an Amazon employee at the time of the incident, it highlights the fact that people with specific or inside knowledge of cloud service providers pose a special risk. This needs to be considered when adopting a cloud migration strategy.

4. Our Recommendations

For any organization that has existing cloud deployments or that is planning to migrate applications to the cloud we recommend the following action items as a result of the Capital One incident:

- Perform manual review of IAM policies and roles for resources and identities. There are automated tools that can help perform a certain amount of policy checking but in general it requires a manual review by experts who understand the use cases and the application context.
- Trace API calls in AWS to find out what IAM roles are used by each application.
- Perform periodic review of deployed IAM roles and policies with automated checking tools to detect any deviations from the specified baseline.
- Execute automated compliance scans to detect any configuration changes of cloud resources.
- Integrate compliance checking into DevOps process.
- Do not allow direct access from front-end web server to data sources. Use protected API's or middle-tier service to access data.
- Deploy WAF that protects against common application layer attacks such as SSRF.
- Encrypt S3 buckets using customer managed keys (CMK) with highly restrictive IAM key policy.
- Monitor cloud logs (AWS CloudTrail) centrally to detect any suspicious behavior.
- Perform penetration testing to identify any potential vulnerabilities.

We ill be happy to discuss in detail the specific requirements for your organization.

Pls contact us sales@holistiCyber.com