Incident Response Plan: BlockTech Cloud Adoption

Project Report

for
Ross Spelman

by
Rohan Bhangale (x18147119)

Contents

Blocktech Overview

Blocktech is a global Finance Technology (FinTech) company, with offices in North America, Europe and Australia, making it liable to the information technology laws, regulations and directives applicable to the continents. These offices have following functions HR, Payroll, Marketing, Service Administration, Services Support, Application Development, IT Systems Administration and Facilities Management. Offices have Windows SQL Databases, Mongo Database, Windows 2012 Server(Physical), AIX Unix Servers, Mainframe (IBM zSeries) and Checkpoint firewalls as underlying IT Infrastructure for the COMMS Room. The workforce comprises of 20 individuals/office and is equipped with Toshiba Protege laptops with Windows 7 OS and iPhone 6. For connectivity wired connection and WIFI is available for internal users and guests. Cloud Adoption of Blocktech is implemented as PaaS.

This report entails the ability of Blocktech *to respond to an incident if cloud adoption is to happen while assessing the impact of Blocktech's Incident Response on cloud adoption move.*

Cloud-based Incident Response Advantages & Disadvantages

Advantages

Reduced Cost

Hosting Incident Response on Cloud helps in reducing the cost of Infrastructure and upgrades in infrastructure, minimizing maintenance costs and training for the IT Staff looking after the Hardware and avoids costs on perimeter security. Billed as per usage.

Added Scalability

At the time of high influx, generally servers were increased to handle logs and events on the On-prem Incident Response Infrastructure but with cloud, the CSP scales up the environment assigns more VPS and increases the capability of the Incident Response with agility simply by upgrading the cloud package.

Added Flexibility

With the move on cloud flexibility and mobility can be achieved as the employees can access the Incident Response Dashboard from anywhere and the ability to access the tools through web overcomes the limitation of the requirement of having a good performance PC.

CSP Data Backup

Initially, with On-Prem Incident Response, backup was kept in order for recovering from a disaster. While with cloud adoption, backup is maintained by CSP so the organisation does not have to look after the backup and recovery process.

Avoided Perimeter Security

With the move on the cloud, the organisation no longer needs to maintain the physical infrastructure which avoids costs required to secure this IT Infrastructure, so no requirement of perimeter security as the Physical IT Infrastructure is looked after by the Cloud Service Provider(CSP)

Collaboration

Cross-Platform collaboration can be achieved as team-members from various geographic locations can interact and work simultaneously and share data, which aids in a performance boost.

Automated and Interactive Procedures

With automated Runbooks and interactive guidance provided by the cloud, the IR team can be assisted and can perform well without panicking in situations of data breaches and attacks

Disadvantages

Lack of visibility

With the lack of security in the picture, the low-level flow of information(network packets) can not be monitored which leaves a window for unidentified indicators of compromise.

Lack of event data

Inability to get data out from the environment, lack of access to the data which flows in underlying hypervisor and network

Lack of access to evidence

Logs and low-level system information are not accessible for forensics analysis and evidence gathering, due to multi-tenant various issues can not be addressed as the agreement with CSP all information can not be accessed.

Missing controls and processes

Most of the tools which are required in Incident Response are not available on the Cloud-based Incident Response dashboard

Skills gaps

The in-house skills do not necessarily help with the cloud-based Incident Response as the team is not experienced and skilled with cloud technology.

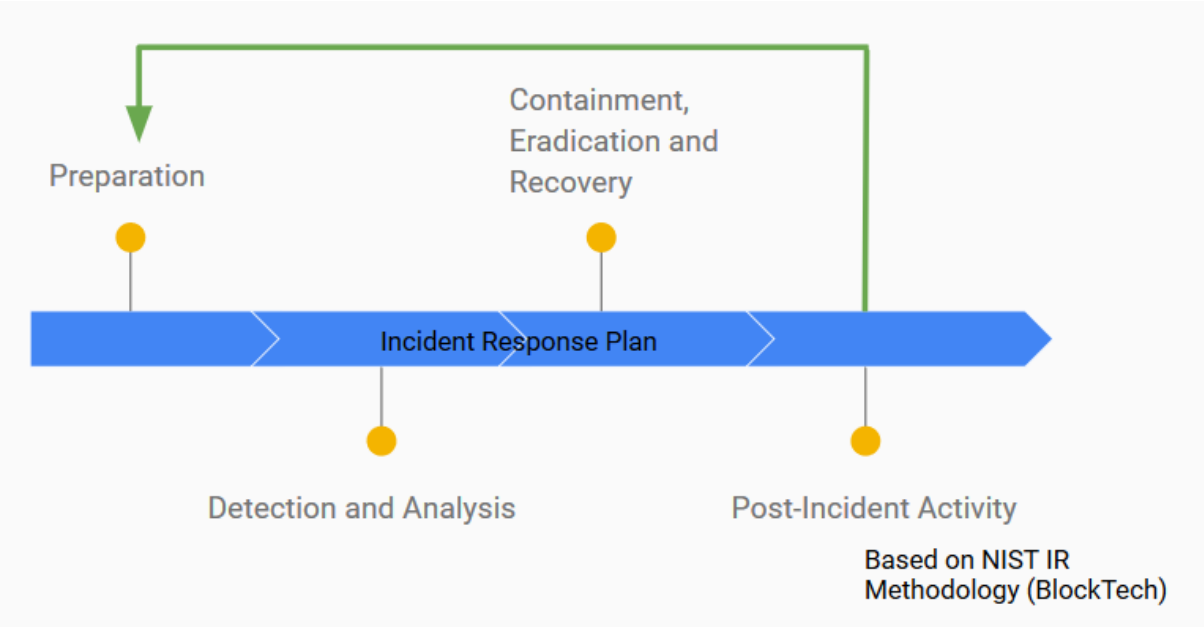
Prone to Attacks

Cloud Infrastructure is prone to attacks such as DOS, exploits carried out by privileged users, vulnerabilities found in hosting environment based on OS, Applications, underlying Network and Hardware equipment and misconfiguration of hypervisor at the event of updates and scaling. Malware intrusion from other tenants of cloud

s

Incident Response Plan

When Incident occurs, Blocktech should have an Incident Response Plan to address data breaches and attacks. To detect, respond and recover from issues like services outages, data loss and cybercrime etc. Using the NIST Incident Response Framework, Incident Response Plan for Blocktech is drafted.



Preparation

- Incident Response Team pre-identify the roles and responsibilities for the IR Team based on the skill sets and authority to make decisions. Roles viz.
    - Director, someone who manages the IR team and is authorised to take a high level decision.
    - Lead Investigator, someone who is in charge of looking after the execution of IR activities in right order and time, also manages Forensic Technicians and Evidence Handlers and interacting with the legal advisor and dispatcher
    - Forensic Technician, someone who is responsible for analysing evidence and reporting findings
    - First Responder, this can be anyone who notices the incident and is responsible to secure crime scenes and collect evidence.
    - Evidence Handler, responsible for handling the gathered evidence and maintaining a strict chain of custody.
    - Legal Advisor, provide guidance and help in pursuing any legal activity.
    - Dispatcher/Helpdesk: First line of contact for reporting Incident, should be available 24*7, responsible for filling IR reports and assigning tracking numbers to new cases

- Carry out information security risk assessment and management with the help of RED and BLUE teams inside the organisation

- Defining ***Severity Index*** based on the type of incident, its commonality and affected parties and potential damage and loss.
- Establishing communication protocols and secure links for facilitating communications
- Establishing WAR ROOM and avoiding the use of corporate emails as they might be compromised
- Building Playbook/Runbooks based on the past incident learnings.
- Training Staff for their IR roles and responsibilities, while carrying out briefings weekly, for creating awareness and educating the staff with current cyber-attacks and scenarios. Conducting cyber incident mock drills. Training such as Secure Human by SANS and Know Before by Kevin Mitnick should be provided to the staff for resilience and vigilance.
- Integrating applicable regulations(GDPR, IRS) and compliance (PCI) to the policies to be followed during the IR Plan.
- Documenting a list of contact information(email, phone) of various IR roleplayers. Furthermore, the Incident Response strategy should be documented with meticulous detail
- Providing training on Cloud Computing and Virtualization.

Detection and Analysis

- Identifying and Validating an attack, being able to distinguish between an ***event*** and ***incident*** using automated and manual detection and classifying and prioritizing.
- Incidence evidence should be ID-ed, protected and reported
- All events should be passed on a SIEM tool for detecting malicious and suspicious activities from AV, Firewalls, IDS, IPS, File Integrity Monitor, System and Network equipment and Application Logs(ie Host and Network-Based Components).
- Data should also be collected from the witness and personal files from individuals.
- Recording Date/Time of occurrence and detection, description, the system involved and associated error messages and name of Identifier.
- While performing forensic analysis, the confiscated equipment(present of CSP Infrastructure), software should be ID-ed with Serial, Arrival and Departure Time, Location and Handler name should be noted. Analysis should focus on identifying the attacker and victims, how was the attack carried out etc.
- Assessing the damage on business and operations and scope of Breach
- Identifying the entry point of the attacker.
- Assigning Severity Index (LOW, MODERATE, HIGH)
- Examine Evidence answering WWWWH? (WHO, WHAT, WHEN, WHERE, HOW)

Containment, Eradication and Recovery

Containment *avoiding further damage from occurring*

- Treating evidence in such a way that it would be admissible in a court of law and chain of evidence is maintained
- Disconnect from Network
- Stop operation

- Disable Accounts
- Perform BackUp on an infected target
- Observe and assess
- Initiate Full System BackUp
- Inform helpdesk
- Change the credentials on affected systems
- Vulnerability analysis to identify the root event and entry point
- Encapsulation of incident occurred
- Carrying out actions necessary to mitigate the incident

Eradication & Recovery *remediating compromised hosts, malware centric. Bringing the affected production system back online.*

- Power off and reboot systems/services for Denial of Service.
- Perform eradication processes pertaining to specific incident type
- Harden OS
- Carry out Recovery
- Apply patches and perform security audits
- Review services and update policies and procedures
- Tighten Access Control List
- Re-install.
- Remove malware code and virus.
- Assess the impact on OS
- Remove dormant UIDs
- Change S/W and H/W Configurations
- Restore from a previously stored backup
- Verify System
- Fill gaps identified during Incident Analysis

Post Incident Activity

Final Stage of IR Process, to conduct a Lessons Learnt Session and Meeting including all the members involved in the Incident Response Team, discussing

- How the Incident Occurred and What triggered it?
- What changes should be made in order to avoid such incidents from occurring in the future?
- How could it have been done better?
- Carrying out interviews and accessing and sharing notes taken during the breach
- Alerting the applicable state and central regulatory bodies
- Which weakness was exploited?
- Areas which need improvement
- Areas where IR Team were effective
- All the learning should be implemented in the Preparation Stage
- All the affected Data Subjects should be informed about the data breach and what information was exposed.

Recommendation to CISO

Establishing joint Incident Response Plan with the CSP
SLA should be signed by the organisation and the CSP backed by shared financial responsibility if SLA is not met. Meeting with the Incident Response Team of the CSP should take place, in order to layout roles and responsibilities and exchanging contact details and backup contact numbers along with secure communication channels. A clear understanding of Incident Response Plan should be there between BlockTech and CSP, for the smooth functioning of the Incidence Response Plan. Identifying and learning about the triggers used for identifying the incident by CSP. Will the CSP give access to physical infrastructure deployed at the Datacenter in case of a physical cyber incident?

Evaluate the security and monitoring controls set in place by the CSP
It is essential to know what kind of surveillance and safety measures are placed by the CSP and what access you have to these tools for an efficient reaction to incident linked to cloud infrastructure. If these tools seem incapable, deploy supplementary fixes for these tools. Deploy Incident Response Plans specific to systems and applications deployed in the cloud.

Building a Recovery Plan
Determine how much data is being stored and where it is stored? How critical it is to the business? And based on that a recovery plan should be created. How often the system is being imaged. Does the CSP have access to the backup data? How much data can Blocktech afford to lose? How quickly the business has to go back up online?
Recovery Plan should state a backup Vendor for cloud as in alternate CSP.

Assess Forensic Tools for Cloud Infrastructure
Evaluating Forensics tools which are at disposal provided by CSP and what other sources are available for carrying out forensic analysis. Evaluating the Forensic Analysis process and how the evidence is being handled during the process. How PII(Personally identifiable information) that potentially identify specific individual, is handled and taken care of with the help of appropriate tools for tracking forensics and evidence trails

Reference/Source

[1]“YouTube.” [Online]. Available: https://www.youtube.com/watch?v=t8AuXEjBzjI. [Accessed: 05-Aug-2019]

[2]“YouTube.” [Online]. Available: https://www.youtube.com/watch?v=ru0-lL09aPc. [Accessed: 05-Aug-2019]

[3]“YouTube.” [Online]. Available: https://www.youtube.com/watch?v=3Vjq-DQDxR4. [Accessed: 05-Aug-2019]

[4]“YouTube.” [Online]. Available: https://www.youtube.com/watch?v=CV-Z5ujuhOQ&t=856s. [Accessed: 05-Aug-2019]

[5]“Incident Response Plan 101: How to Build One, Templates and Examples,” Exabeam, 21-Nov-2018. [Online]. Available: https://www.exabeam.com/incident-response/incident-response-plan/. [Accessed: 05-Aug-2019]

[6]“3 Steps for Effective Information Security Event Triage [Infographic],” Rapid7 Blog, 13-Dec-2016. [Online]. Available: https://blog.rapid7.com/2016/12/13/the-three-steps-for-effective-information-security-event-triage/. [Accessed: 05-Aug-2019]

[7]“Incident response process in a cloud environment,” SearchCloudSecurity. [Online]. Available: https://searchcloudsecurity.techtarget.com/tip/Incident-response-process-in-a-cloud-environment. [Accessed: 05-Aug-2019]

[8]“Data incident response process | Documentation,” Google Cloud. [Online]. Available: https://cloud.google.com/security/incident-response/. [Accessed: 05-Aug-2019]

[9]rkarlin, “Respond to security incidents with Azure Security Center.” [Online]. Available: https://docs.microsoft.com/en-us/azure/security-center/security-center-incident-response. [Accessed: 05-Aug-2019]

[10]“Faster Incident Response through Automation,” Salesforce.com. [Online]. Available: https://www.salesforce.com/video/306691/. [Accessed: 05-Aug-2019]

[11]K. McCracken, “10 Steps to Develop an Incident Response Plan You’ll ACTUALLY Use,” Medium, 28-Feb-2018. [Online]. Available: https://engineering.salesforce.com/10-steps-to-develop-an-incident-response-plan-youll-actually-use-6cc49d9bf94c. [Accessed: 05-Aug-2019]

[12]“Future-proof your incident response plan.” [Online]. Available: https://www.charteredaccountants.ie/(X(1)S(1d15p1cuez3kvjchasb5xqap))/Accountancy-Ireland/Articles2/Spotlight/Latest-News/future-proof-your-incident-response-plan?AspxAutoDetectCookieSupport=1. [Accessed: 05-Aug-2019]