CYBERSECURITY CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana

The Hague Centre for Strategic Studies

Den Haag

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Kingdom of the Netherlands

Compromised Data Centre and Cloud Infrastructure

Incident Overview:

Company: CyTrex Global Solutions
Industry: IT Services and Software Development
Location: Global (HQ in the US, with cloud services hosted in the EU)
Incident Date: 12th October 2024
Discovery Date: 14th October 2024

Cynor Sense
Experience Safety

Incident Story:

CyTrex Global Solutions is an IT services company managing large volumes of customer data. On the morning of October 14th, CyTrex's Security Operations Center (SOC) detected unusual outbound traffic patterns from the company's primary data center in Europe, along with irregular access patterns to cloud-hosted services. The data center hosts critical client applications and data storage for financial and healthcare sectors.

A subsequent investigation by the SOC team revealed that the attackers had exploited an unpatched vulnerability in the data center's firewall (CVE-2024-XXXX), allowing them to escalate privileges. From there, they gained access to cloud-based services through compromised administrative credentials, where customer databases and proprietary software were hosted.

Within 72 hours, CyTrex's leadership team realized the extent of the breach: attackers had exfiltrated sensitive customer data, including financial records and personal information. The attackers also deployed ransomware on cloud-hosted virtual machines, demanding a large sum in cryptocurrency in exchange for restoring the encrypted data. Several services for healthcare clients were down, which led to disruptions in operations.

Despite SOC efforts to contain the breach, the attackers had already gained control over several systems. At the time of discovery, backups were also found to be encrypted by the ransomware. The company's Incident Response (IR) team was activated, and third-party forensic experts were engaged to understand the full scope of the attack.

Key Events in the Incident:

- **Oct 10th:** Firewall misconfiguration left a known vulnerability (CVE-2024-XXXX) exposed. No patching or updates occurred due to administrative oversight.
- **Oct 12th:** Attackers exploited the firewall vulnerability, escalating their privileges within the data center and accessing cloud systems.
- **Oct 13th:** Attackers moved laterally, compromising the backup systems and encrypting critical data, including customer records.
- **Oct 14th:** The SOC team detected unusual network traffic, triggering the incident response protocol. However, containment efforts were delayed due to internal communication gaps and a lack of incident playbook testing.

- **Oct 15th:** Ransomware demand was received, asking for 100 Bitcoin to decrypt the affected systems and avoid further data exposure.

Tasks for the Team:

1. Task 1 : Identify Policy/ Governance Faliures

- What gaps in cybersecurity policy or framework do you see that allowed this incident to occur?

2. Task 2 : Identify TTPs ,

- Based on MITRE ATT&CK, NIST 800-61, or any other frameworks, identify potential tactics, techniques, and procedures (TTPs) used by the attackers. How would you strengthen defenses to prevent such attacks in the future?

3. Task 3: CERT-IN Breach Notification and other regulatory Implications

- Based on India CERT-In guidelines, what are the key steps that need to be taken to comply with breach notification regulations? How should GDPR be addressed, considering the European data storage involved?
- Identify any potential regulatory, financial, or reputational penalties that the company might face due to the breach. How should the legal team handle potential lawsuits or contractual breaches with clients?

4. Task 4

- **IR Team:** How would you apply the NIST 800-61 Incident Response Lifecycle (Preparation, Detection & Analysis, Containment, Eradication, and Recovery) in this scenario to improve coordination and response times.

Deliverables :

- Create a comprehensive presentation covering all the above 4 Tasks
- Create a video byte explaining the approach and your PPT not exceeding 3 minutes.

Contributors:

CynorSense Solution Pvt. Ltd. is a trusted partner in cybersecurity, committed to providing tailored, cutting-edge security solutions for businesses of all sizes. With expertise in Penetration Testing, SOC & SIEM Services, and comprehensive security assessments, they help clients protect digital assets and maintain compliance with industry standards. CynorSense combines innovative technology with in-depth cybersecurity knowledge to offer reliable protection in an ever-evolving threat landscape. https://www.cynorsense.com/