City of Dallas

After Action Review Report (AAR) of May 3rd Ransomware Incident

Dallas City Council
September 20, 2023

Dr. Brian Gardner
Chief Technology & Information Security Officer
Department of Information and Technology Services
City of Dallas

Presentation Overview

- Background/History
- May 3, 2023
- City Operational Impact
- Impact Mitigation
- Recovery
- Acknowledgements
- Findings
- Recommendations
- City Investments

Background/History

April 7-May 3, 2023

- Royal Group performed
  - Reconnaissance &
  - Staging
- Less than 1 month
- Leakage of 1.169 TB of the 3.8 PB data the City has

Background/History

Reconnaissance

- Exfiltration of Data
- Command-and-Control Beacons
- Preparation to Deliver Encryption to Files
- Review of Users (Who is Who)

Background/History

- 70% of Organizations suffer Ransomware
- 100% surge from the second quarter of 2022
- Mean time to identify a data breach is 204 days
  - City identified in 27 days
- Mean time is 73 days to contain breaches
  - City contained in 1 day

May 3, 2023

- Use of Service Account
- Threat Actor Begins Encrypting Files
- Ransom Request Files Found On 996 Hosts
- Incident Response Plan (IRP) Activated
- Multiple Incident Response Teams Activated
  - Internal Teams
  - Vendors
  - Cybersecurity Professionals
- Mitigation Efforts Initiated & Paused

City Operational Impact

- Interruption to All City Operations
  - All City Departments
  - Impact
    - Public Safety
    - Public Facing Services
    - Technology Infrastructure

Recovery

- May 3, 2023
  - Focus on Eradication
- May 4, 2023
  - Last known Infection
- Full Recovery Work Began
- Priorities set Based on Previous IRP
- Communication to State & Federal Authorities

Recovery

- Information provided to Law Enforcement
- Incident Support Team (IST)
- Multiple Remediation Team working in Coordination
- City currently has 14,000 assets
  - 230 Server
  - 1,168 Workstations
    - Less than10% of assets infected

Recovery

- Over 90% restoration by June 9, 2023
- Currently 99.9% restoration
    - Small portion of
        - Test
        - Development
        - Unsupported systems needing upgraded
- Removed 100 servers of technical debt

Acknowledgements

- Dallas Fire Rescue
- Dallas Police Department
- Office of Emergency Management
- GTS
- State & Federal Agencies
- Outside Vendors

Findings

- Incident Response Plan Revisions
- Security Incident Staff Periodically Exercised
- Identification/Detection of Threat
- Aggressive Incident Response
- Substantial Cybersecurity Investments Made in Advance of Attack

Recommendations

Plan of Action & Milestones

- Cybersecurity Program Review
- Privacy and Security Risk Assessments
- Backup and Recovery Processes
- Network Hardening
- Actively Manage Infrastructure and Software
- Update to the Incident Response Plan

Impact Mitigation

- Increased in Information Security Budget
- Periodic Reviews by Federal and Outside Organizations
- Addition of Zero Trust Technologies

City Investments

Cybersecurity Spend

- 2019 2.5% of the total ITS budget
- 2023 ~10% of the total ITS budget
- Innovative Technologies
- Strategic Plan
- $8.5 million in computer-based interdiction, mitigation, recovery, and restoration efforts

City of Dallas

After Action Review Report (AAR) of May 3rd Ransomware Incident

Dallas City Council
September 20, 2023

Dr. Brian Gardner
Chief Technology & Information Security Officer
Department of Information and Technology Services
City of Dallas