RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **PDAC-T11**

How to protect your enterprise data (tools and tips)

Jeff Streelman

Data Protection Program Director

#RSAC

Abstract

Today firms need to take a holistic approach to identifying and protecting their sensitive data.

As data is everywhere, this session will look at protection of data in the enterprise, on the network, in the cloud, and in applications.

There is no single answer to data protection but in the face of growing privacy regulations, firms must demonstrate compliance.

Introduction

From this session, you should take away tips for Data Protection

. . . and Privacy Regulations

. . . in the Enterprise

. . . on the Network

. . . in the Cloud

. . . in Applications

Data Protection and Privacy Regulations

Data Protection and Privacy Regulations

- Everything begins with good corporate and work force policies
  - Demonstrating compliance starts with having a documented policy
  - Check out http://oecdprivacy.org/ for 8 “Privacy Principles”

① Establish a Data Protection Policy / Standard

- Over communicate to your workforce!
- Make it know that it is everyone's responsibility
- Partner with HR, Legal, and Compliance when establishing your policy

8 Privacy Principles

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle → reasonable ways to reduce risk
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

Credit: http://oecdprivacy.org/

Data Protection and Privacy Regulations

- Practice good data hygiene
  - Establish a data retention policy and communicate it (often) to your workforce!
  - Remove the data when you are done with it

② Sponsor a company “Digital House Spring Cleaning Day” annually

  - Ask senior managers to set the tone
  - Encourage managers to push this message down to their staff
  - Work with your HR, Legal, and Compliance departments
  - Use the days before the event to provide training and awareness
  - Do this at home too – does your town sponsor shredding days?

Data Protection in the Enterprise

Data Protection in the Enterprise

- Classic Data Leakage Protection (DLP) software goes here
  - When were your DLP policies and thresholds last reviewed by senior management?
  - Do your policies accurately reflect your firm's risk tolerance for data leakage?
  - Are you monitoring the most common data leakage vectors – email, web uploads, USB write, FTP transmissions, off network activity?
  - Are all your documents classified and does your DLP system utilize those tags to improve detection and protection?
  - Does your company block data from exfiltration or just monitor?
  - Does your company publish metrics to demonstrate compliance?
- Call to action if you ask yourself these questions and you're not comfortable with your answers

Data Protection in the Enterprise

③ Make patching a priority (establish zero tolerance)

- Know your inventory and relentlessly patch everywhere (infrastructure, software, middleware, APIs, etc.)

④ Make the ability to send/receive external email a privilege

- Why does every worker need the ability to use external email?
- According to the Verizon DBIR (Data Breach Investigations Report), 94% of malware was delivered by email; 23% by web!

Data Protection in the Enterprise

⑤ Establish a repeat offender process for data leakage events

- Establish consequences for data leakage
- Make management aware of their workers incidents

⑥ Wherever possible, lock it down (web sites, USB access, FTP, off-network access)

- Not everyone needs to use these services, so why allow them by default?
- Does your company have a speed bump for unclassified web pages?

RSAConference2020

Data Protection on the Network

Data Protection on the Network

- Most organizations run complex networks based on Microsoft Windows Servers which utilize Active Directory

  ⑦ Implement a Microsoft Active Directory Red Forest to protect all privileged domain accounts

- Identify and lock down all functional IDs, especially privileged IDs!
- Scan regularly for Open Shares and lock them down!
- Create a dedicated employee Wi-Fi and Guest network separate from your production network
  - Only allow vendors access for limited durations to Guest network

Data Protection in the Cloud

Data Protection in the Cloud

- Companies are embracing the cloud at different speeds
  - Cloud security is a joint effort between the cloud provider and company
  - Understand what clouds services are in use at your company and what data is being stored in the cloud
  - Keeping the data secure means establishing the right controls and “guard rails” so that any breach is quickly detected and contained

⑧ Always encrypt your data in the cloud and keep your keys separate and secure

RSAConference2020

Data Protection in Applications

Data Protection in Applications

- Data is generally more well protected inside applications where only authorized workers have access

⑨ Review authorizations of your workforce regularly, especially privileged access to your applications and infrastructure

- When data leaves the protected boundaries of the application, it becomes “unstructured data” which limits the controls that are in place

⑩ Reduce the amount of unstructured data by putting limits on the amount of data that can be exported by an application

RSA Conference2020

Summary

Summary of TIPS (page 1)

① Establish a Data Protection Policy / Standard

② Sponsor a company “Digital House Spring Cleaning Day” annually

③ Make patching a priority (establish zero tolerance)

④ Make the ability to send/receive external email a privilege

⑤ Establish a repeat offender process for data leakage events

Summary of TIPS (page 2)

⑥ Wherever possible, lock it down (web sites, USB access, FTP, off-network access)

⑦ Implement a Microsoft Active Directory Red Forest to protect all privileged domain accounts

⑧ Always encrypt your data in the cloud and keep your keys separate and secure

⑨ Review authorizations of your workforce regularly, especially privileged access to your applications and infrastructure

⑩ Reduce the amount of unstructured data by putting limits on the amount of data that can be exported by an application

Apply What You Have Learned Today

- Next week you should:
  - Discuss Tip #3 (Make Patching a Priority) with your CISO/CIO
- In the first three months following this presentation you should:
  - Have a detailed plan of attack regarding patching
  - Perform an internal review of your DLP program and discuss policies and risk tolerances with senior management
- Within six months you should:
  - Completed review of all 10 tips with CISO/CIO and prioritize

RSAConference2020

Thank You!