Data Security Strategies in Data Center Environment

Presented By –
Meetali Sharma

Equifax

Petya

WannaCry

CloudBleed

Bad Rabbit

Report Snapshot

Who's behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Who are the victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

Quick Takeaways

Be vigilant
Log files and change management systems can give you early warning of a breach.

Make people your first line of defense
Train staff to spot the warning signs.

Only keep data on a "need to know" basis
Only staff that need access to systems to do their jobs should have it.

Patch promptly
This could guard against many attacks.

Encrypt sensitive data
Make your data next to useless if it is stolen.

Use two-factor authentication
This can limit the damage that can be done with lost or stolen credentials.

Don't forget physical security
Not all data theft happens online.

Source: Verizon - 2017 Data Breach Investigations Report

Data Security Strategy

- Conduct Risk Assessment of Data Center
  - Threat Landscape
  - Existing Controls
  - Security Posture
- Conduct Third Party Risk Assessment of Data Center

Physical Security

- Fire
- Humidity
- Temperature
- Building Perimeter

Access Control

- Two-factor authentication
- Virtualization

Hardware

- Redundancy

Insider Threat Protection

- Training
- Incident Management

Server Security

- Anti-Virus
- Patch
- Vulnerability Management
- DLP

Regulatory Compliance

BCP/DR

- Backup Restoration Tests

Countermeasures

Physical Security

- Have a secure physical location
- Surveillance cameras
- Fire resistant walls
- Install Intrusion alarm systems
- Temperature and humidity monitoring
- Fire Safety
- Continuous Power Supply and backup
- Preventive maintenance checks

Access Control

- Secure access to authorized personnel
- Two-factor authentication
- Give access as per role
- Have virtual connections to servers
- Logs inspection

Countermeasures

Server Security

- Use Intrusion Prevention System (IPS)
- Secure connections to server
- Identity management
- Ensure regular –
  - AV updation
  - Patching
  - Vulnerability assessment

Hardware

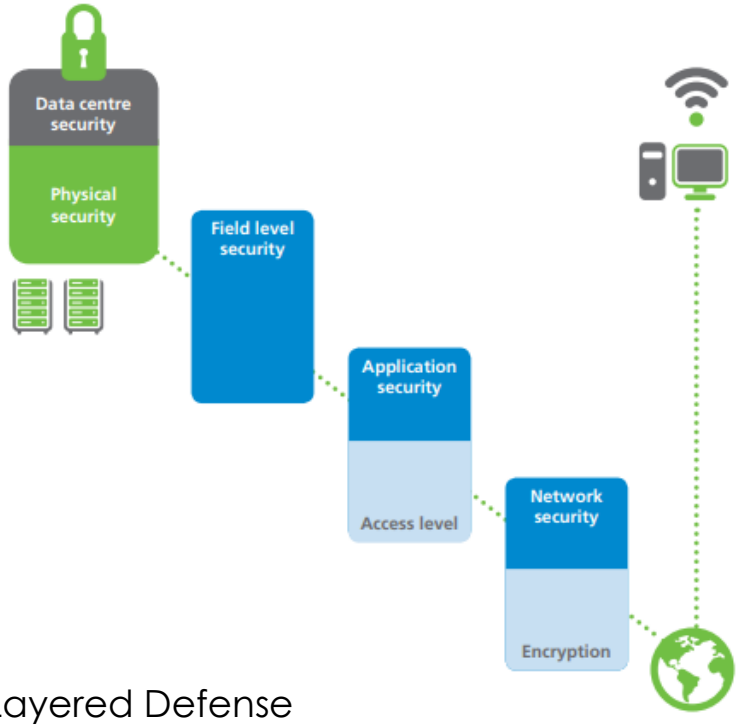
- Have backup hardware
- Secure storage of backup tapes
- Encrypt data
- Separate web server and data server

Data Centre Security

Countermeasures

BCP/DR

- Have a second datacenter
- Conduct backup restoration drills



Layered Defense

Access Control

- Secure access to authorized personnel
- Two-factor authentication
- Give access as per role
- Have virtual connections to servers
- Monitor connections to server
- Have protective technologies - malware protection, host intrusion prevention, and data loss prevention
- Remove default accounts
- Isolate from parent network where required

Countermeasures

Insider Threat

- Regular training of personnel
- Monitoring of activities
- Conduct background checks
- Define and test Incident Management Process

Design Security framework and architecture

- Overall security goals
- Level of security required
- Security standards to be implemented
- Auditing & monitoring strategy
- Definitions of Training & Processes to be implemented
- Regular Risk Assessments and controls optimization to build threat resilience

Stay Secured, Protect Data

Thank You

Contact Details –

Meetali Sharma
meetalisharma81@gmail.com; meetali.arora@sdgc.com
+91-9971393639