ISACA
Serving IT Governance Professionals
Greater Houston Area Chapter

That 4th Quarter Security Review

SENTIGY℠
EXPERIENCE THAT COUNTS

Introductions

- Roy Wood
  - Senior Security Consultant
  - CISSP, CCNA, PMP
- Tom Fluker
  - Service Delivery Manager
  - PMP, Six Sigma Black Belt

What is a security review?

- A comprehensive look at networks, applications, data and processes associated with data protection
- Includes
  - Reviewing IP schemes
  - Network architecture and devices
  - Penetration testing
  - Security awareness
  - Policies and procedures

What is important?

- Do we know where all the important data is stored?
- Is data protected at all times, at rest, in transit and in use?
- Is data at rest on mobile systems protected?
- Is the data classified?
- Are laws from other countries a concern?
- Is data held by third parties protected?
- Are there physical vulnerabilities?
- Are there logical vulnerabilities?

What tools do we use?

- Nessus
- Nmap
- Observation
- Log Reviews
- Social Engineering
- Process Mapping
- Wireless evaluation
- Various attack simulation tools
- Guidelines from the various standards organizations
  - FERC, NERC - CIP, HIPPA, JCAHO, PCI, ISO, GLBA, SOX (CoBIT, COSO)

Questions we ask regarding for external protection

- Do we have a standard for external hosting?
- Do we have a standard for third party access?
- Do we have a standard set of questions for vendors and hosting facilities?
- Ask for scan reports
- Ask for certifications – SAS70 type 1 or 2, ISO, PCI
- Can we scan external sites?
- What are the procedures internally for the vendor hosting our data?
- Who handles this data?
- Where is it backed up?
- Who owns data, how do we get it?

What are we looking for?

- Signs of intrusion
  - Suspicious access
  - Repeated failed attempts to login
- Account escalation
  - More authority than before
  - New accounts
- Malware, viruses, etc
- Known and unknown attack vectors
- Patch levels
- Appropriate network design for the organization
  - This is not a “one size fits all” situation
  - Understanding risk and the appropriate mitigation steps are personal
- Physical access to equipment and space
- Security awareness and understanding

Why are we doing this?

- Pass the audit or “because the policy says so” seems to be the most stated reason
- The real reason – Data Protection
  - However, many organizations will not proactively work on security on their own
- Goals
  - Find issues before they become a problem
  - Plan a path forward for future projects and training
- Differs from an audit
  - Remediate or Celebrate is an IT perspective on audit
  - Security reviews provide new ways to address issues or new thoughts altogether

Why are we doing this?

- In a recent Ponemon Instutite study, only 16% CEOs are very confident they will not have a data breach in the next 12 months.
- 82% of those in the study did have a data breach in the last 12 months.
- The estimated cost is $200 per compromised record

What are the benefits?

- Fines avoidance
- Improved Asset performance
- Reputation management
- Income protection and stock value protection
- Reduce data breach recovery costs
- Reduce customer turnover
- Reduce employee turnover

What data is critical?

- Customer information
- Employee information
- Financial information
- Non-financial, business information
- Intellectual Property

This is presented in the order that CEOs feel the data is most difficult to secure. Generally, the need for data accessibility is what drives this difficulty. Customer data is in the most demand, so it becomes the most difficult to secure.

Common Issues

- eMail and IM are significant issues of data loss
- Technical staffing
  - Critical path individual
  - Business continuity is keyed one person
- Absence of documentation
- Segregation of duties
  - Not just an issue in financial departments
- No understanding of data classifications
- Tools in use
  - They may be there, but without monitoring them, it does not help
- Network architecture
  - DMZs are commonly installed, but not always effective in design or deployment

ISACA®
Serving IT Governance Professionals
Greater Houston Area Chapter

Things to Consider

- Mobility and access
  - How do you allow accessibility without compromising security
- Data ownership
  - It is not as simple as you think
- Cloud computing
  - Issues may arise regarding security, data ownership and discovery

Summary

- What needs to be done
  - Develop a data protection strategy
    - Decide on what constitutes a secure network in your environment
  - Employee training
  - Reduce security flaws in business applications
  - Instill management ownership of security
    - Most CEOs are NOT out of touch on this. Good dialog and planning can greatly enhance security

Questions?

Data Sources

New Ponemon Study Reveals Disconnects in Building the Business Case for Data Protection

SPEAKERS:

Jack Danahy, Security Executive, IBM (Former Founder & CTO, Ounce Labs)
Dr. Larry Ponemon, Chariman & Founder of The Ponemon Institute

Retrieved from http://event.on24.com/eventRegistration/EventLobbyServlet?target=lobby.jsp&playerwidth=950&playerheight=680&totalwidth=800&align=left&eventid=165047&sessionid=1&partnerref=bizcard&key=67614A80BEA68D243623EAED25C2C5A1&eventuserid=30013221 on November 11, 2009

ISACA
Serving IT Governance Professionals
Greater Houston Area Chapter