Investigating the legacy system challenge of Internet connectivity.

A case study.

Presented by: Martin Norman
Director, Technical Services

www.safestone.com
About SafeStone

- Premier IBM Partner for AS400 / iSeries Security for 15 years
- Member of IBM World Wide Partner in Development Program
- Over 1,500 security software installations world wide
- Headquarters in Princeton, New Jersey with offices throughout the world
Presentation Agenda

- Define the challenge facing the client
- Describe the investigation / audit process
- Summarize the findings
- Itemize the main recommendations
- Conclusion – lessons to be learnt
Legacy environment

- iSeries 400
- Inventory optimization application
- Minimal OS/400 expertise
- No security expertise on iSeries 400
- Security policy in place but not formally applied to the iSeries 400
The challenge!

- Their software provider has developed a collaborative portal for e-business
- The client’s own vendors will now get Internet based connection into the iSeries 400
Step 1 – authenticate
Step 2 – select partner
Step 3 – URL and token issued
Step 4 – connect to partner
Step 5 – check token back to portal
Step 6 – check inventory
The challenge

- How secure is the iSeries 400?
- What could these new users do?
- Project was critical to new corporate initiatives – it had to work
- The only people with knowledge of how the legacy application worked were also the portal provider
The investigation / audit process
Methodology

- Interview
- Compliance audit
- Event auditing
- Exit point checking
- Being inquisitive
Interviews

Who:
- Power users
- Help desk
- Operations personnel
- Security officer
- Auditors
- Application owners
- Application developers
Compliance audit

- System values
- Network attributes
- Profile parameters
- Library contents
- Authorities
- OSRs
Event auditing

- Extract security events from OS audit logs
- Profile changes
- Program adopts
- Authority failures
- Ownership changes
- Signon errors
Exit point checking

- Monitor requests through the security exit points
- ODBC
- Remote commands and programs
- FTP
- TELNET
- SQL
- File transfers
Findings
Findings

- Back-door to command line
- Help desk with “all object” authority
- System auditing was not in use
- System values were not enforcing corporate policies
- Exit points not being used
Findings ctd.

- 38 versions of application libraries
- Object authorities allowed *ALL users
- Software developers controlled the promotion / introduction of live changes
- Help desk confirmed who a “user” was on the phone by checking caller ID
Profiles

- Wide variety of abuses found:
  - Old profiles (70 never signed on)
  - Too much authority
  - Non-expiring passwords (many users!)
  - “Package profiles” with default passwords
  - Generic profiles
  - Signon password stored in application client
  - QSECOFR used too regularly
Recommendations
Recommendations: general comments

- Best practices – ISO 17799, GSD 331
- Use a security management tool to simplify administration of the enhanced security
- Appoint an application “owner”
Recommendations: profiles

- RBAC – Role Based Access Control
- Developer to recommend good authority structure
- Strict profile deletion procedures
Recommendations: libraries

- Reduce number of libraries
  - To free up space
  - Less likely to be copies of live data.
  - Security will be easier to manage
  - It is less likely that a “rogue” program exists
  - It is sometimes difficult to identify the correct version of an object or source
Recommendations: others

- Strict change control procedures
- Check for security events daily
- Interface some OS/400 events into their existing Intrusion Detection System
- Help desk users should be given a menu with the necessary commands on it
- Reference the security policy & warnings on signon screen
Recommendations: portal project

- Insist upon a very strict agreement about partners profiles
- Special password structures
- Terminal based authentication
- Monitor requests through the exit points (phase 2 of the project would introduce the control of these requests)
Conclusion

- Whether your partners connect to your legacy applications or not - get your house in order
- Secure your data
- Control access
- Audit the security events
- Monitor the unusual and critical aspects of your systems
- Ensure reports are small enough to be useful
Conclusion

- Have a usable, OS specific, security policy
- Keep the policy current
- Educate your users
- Be wary of the implications of your actions
- Don’t assume – CHECK!
For more information contact SafeStone:

Visit our web page:
www.safestone.com

Contact us via e-mail:
enquiries@safestone.com

Contact me via e-mail:
mnorman@us-safestone.com