Digital Pearl Harbor and the Grid

2nd North American Energy Standards Board ANNUAL MEETING

SEPTEMBER 16, 2003
Austin, Texas

Presented by: Paul.Pechersky@sbcglobal.net
214-340-1144

Overview

- The U.S. Naval War College hosted a war game entitled “Digital Pearl Harbor”
- Purpose was to determine the feasibility of cyber attacks crippling the U.S. economic and national infrastructure.
- More than 100 industry participants representing:
  - Electric Power
  - Financial Services
  - Internet
  - Telecommunications

Presented by: Paul.Pechersky@sbcglobal.net
214-340-1144

Electric Power Industry Scenario

1. Focused on a few markets, rather than attempting a nationwide or even regional outage.

2. A two-pronged approach:
   a) a physical attack against up to 24 transmission towers at key points in three markets,
   b) A cyber attack against three to six SCADA systems in the same markets.

3. First to cause confusion and uncertainty

Presented by: Paul.Pechersky@sbcglobal.net
214-340-1144

Electric Power Industry Scenario (cont'd)

4. Then to disrupt power in key markets

5. Disable key control systems for extended periods.

6. Amplify the effects of the attacks planned by the other industry groups

Presented by: Paul.Pechersky@sbcglobal.net
214-340-1144

Principles

- Participants focused on building a hypothetical scenario for a cyber attack, but several principles for cyber defense also emerged:

1) Enterprises can get into trouble if they develop plans to combat only certain threats, such as hacking

2) Enterprises must view even minor problems as potentially contributing to a wider attack.

3) The vulnerabilities identified could be plugged by good enterprise cyber security practices

Presented by: Paul.Pechersky@sbcglobal.net
214-340-1144

Overall Conclusions

- Improved software security, software quality and personnel reliability safeguards could address most vulnerabilities identified in the war game.
- One problematic issue is the ready availability of information in open sources that terrorists can access.
- Attacks against isolated infrastructure, such as the control systems for electrical power distribution or telecommunications, were more difficult to effect, but at the same time may prove more difficult to detect.
    - We still don't know who caused the NE Blackout!!

Presented by: Paul.Pechersky@sbcglobal.net
214-340-1144

Overall Conclusions

- Attacks against IT networking and financial services systems are easier to effect but are also more readily thwarted by just taking reasonable security precautions.
- Cyber terrorism defense requires a central coordination role that only the U.S. government can provide.

Presented by: Paul.Pechersky@sbcglobal.net
214-340-1144

Macro Conclusion's regarding the Grid

- Cyber attacks alone can't bring down major segments of the electrical system but could cause interruption within regional power grids

- Exposure to cyber-terrorism and associated attacks continues to increase, and the industry has been slow to respond to the increasing threats.

Presented by: Paul.Pechersky@sbcglobal.net
214-340-1144

Relevant Utility Industry Trends

1. Control networks continue to move from analog and electromechanical technology to digital technology.

2. SCADA equipment tends to converge on industry standards and is moving away from proprietary specifications.

3. The need for real-time information about the state of the grid makes more control information available.

4. Security measures within the SCADA and command and control elements of the nation's utilities vary widely.

Presented by: Paul.Pechersky@sbcglobal.net
214-340-1144

Conclusion - Grid

- No single attack will likely cause anything other than an isolated outage.
- Terrorists can't just sit in front of PCs and bring down the U.S. power transmission system.
- Likely scenario requires some inside help combined with a physical attack.

Presented by: Paul.Pechersky@sbcglobal.net
214-340-1144

Conclusion (continued) - Grid

- The widely held belief that critical systems, such as SCADA can be easily accessed remotely is a myth.
  - BUT this is rapidly changing as more standards-based systems replace older technology.
- The industry has been slow to respond to the increasing threat of Cyber Attacks.
- Utilities have deployed only the most rudimentary security services and devices to protect the command and control elements.

Presented by: Paul.Pechersky@sbcglobal.net
214-340-1144

Recommendations - Grid

- SCADA security should be in proportion with the threat.
- Power companies should add protection to transmission corridors
- The Federal government should provide the industry with a set of guidelines on access to information, physical access, and security measures and processes

Presented by: Paul.Pechersky@sbcglobal.net
214-340-1144

Recommendations - Grid

- The industry must adopt a set of security objectives and standards that continue to mature as threats evolve.

- Utilities should be prepared to go beyond what the regulatory agencies require.

Presented by: Paul.Pechersky@sbcglobal.net
214-340-1144