Twenty Secure Computing Recommendations

Our global Information Technology (IT) Infrastructure is under attack, as never before, by professional criminal organizations, terrorist groups and national entities. We must defend our intellectual property, personal data, military secrets and national infrastructure (energy, communications, transportation, water and sewage and other). We must take action now! The list below is far from complete.

1. Know that all or a portion of your IT infrastructure and the global IT infrastructure is likely to be compromised and act accordingly.
2. Understand all current commonly used hardware and software has vulnerabilities.
3. Avoid “gray market” hardware and software. Buy from well vetted vendors and contractors. Prohibit the use of unauthorized subcontractors.
4. Put in place and maintain effective, user friendly, physical security.
5. Train yourself and all organizational personnel on security best practices and organizational policies. Train users to recognize “spear Phishing” and social engineering threats.
6. Evaluate and understand the tradeoffs between security and functionality.
7. Establish and enforce clear, unambiguous security, authentication and privacy policies. Train and retrain periodically all users. Document the training.
8. Review your enterprise architecture for hidden vulnerabilities, unauthorized applications and rogue connections to outside networks including unauthorized/unsecured wireless access points.
9. Make “maximum security” your default IT setting on all hardware and software.
10. Understand no software or hardware is totally effective or cannot be compromised.
11. Monitor all inbound and outbound network traffic plus traffic between internal networks for data leakage, traffic going to unauthorized or known “bad” IP addresses. Create high security zones within internal networks to protect high value data. Set up and monitor “honey pot” PCs.
12. Use WPA v, 2.0 to secure wireless networks. WEP and WPA v1.0 have been broken.
13. Monitor all wireless networks real time on a 7x24 basis.
14. Keep all software and firmware patched. In larger organizations try to evaluate patches for stability and conflicts with existing applications.
15. Assume all external partners’ networks are compromised and that they do not maintain your level of security.
16. Think long and hard before adopting “Web v.2.0” social networking applications for organizational and customer use.
17. Create and exercise - at least every six months - Continuity of Operation Plans (COOP) and Disaster Recovery plans.
18. Monitor the SANS “Internet Storm Center” and other security resources.
19. Understand and develop organizational policies for using removable media.
20. Plan for the unexpected – it will happen! A little professional paranoia is a good thing.
Security Resources and Reports

National Institute for Standards and Testing (NIST)

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-39 (Risk Management)
- NIST Special Publication 800-37 (Security Authorization)
- NIST Special Publication 800-53 (Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment)
- NIST Special Publication 800-60 (Security Category Mapping)
- NIST Special Publication 800-122 (Confidentiality of PII)

NIST has many other IT security resources available.

US-CERT (United States Emergency Computer Response Team)
http://www.us-cert.gov/

“Securing Cyber Space for the 44th Presidency” – Center for Strategic and International Studies (CSIS)
http://www.csis.org/component/option,com_csis_pubs/task,view/id,5157/

“National Cyber Security Research and Development Challenges” – Institute for Information Infrastructure Protection (I3P)
www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf

SANS Internet Storm Center  http://www.sans.org/ (the SANS website is an excellent internet security resource.)

Dark Reading – InformationWeek  http://www.darkreading.com/


http://www.businessweek.com/magazine/content/08_48/b4110072404167.htm
(see previous stories in this series)

Armed Forces Communications and Electronics Association (AFCEA) (training and white papers)  http://www.afcea.org/

George W. Welles
Imaging Futures, Inc.
952-936-9730 (main)
gwelles@imagingfutures.com
http://www.imagingfutures.com