

STATE INFORMATION SECURITY OFFICE

Mainframe

- State CIO Security Officer visited with ITE mainframe staff
- One reason they use SSN is that they need something to match against payroll
- Mainframe staff acknowledge it is a process that has been in place for a long time and are open to new ideas
- Would like something that does not require them to do a lot of programming
- CIO Council discussed using Driver's license instead of SSN also discussed using State ID numbers (from building access cards)
- Building access cards was not a good idea for a number of reasons
 - Not all staff in outlying offices have a state ID card
 - Dept of Public Safety is responsible for the state ID cards and controls if they will continue to use the same type of cards
 - There are three different types of numbers distributed with state ID cards so the numbers are not consistent, which could create some difficulty with administering in mainframe
- Driver's License number was the "winner" in terms of changing our process
 - Still issues to see if can be resolved:
 - Will DOT allow state to use the numbers for mainframe access (Greg will check with Steve Gast to see if this is possible)
 - Not every person has a driver's license; what if an individual just has an ID. Will that individual be able to get a number similar to a Driver's License number?
 - Using driver's license numbers will not require ITE mainframe staff to do any reprogramming, since the data already exists
 - If implemented, this will be a process to make change; probably will do by attrition, ie when new employees enter the workplace, they will use the new driver's license requirements for mainframe access. Those who are already employed, will slowly be switched over to the new system, mostly by attrition
- Next question is how do we match up with payroll:
 - If do use DL, will also need to match up with payroll but may be able to use only last 4 of SSN instead of the entire number. Would that be acceptable? Most in the room agree it would be better than what we have now, which is entire SSN and mother's maiden name.
- Security CIO did acknowledge that while this is a better system than what we currently have, it may be a system that will only be a good solution for the next 10 to 15 years; as technology changes and continues to get more sophisticated
- Security CIO did also acknowledge that other states are struggling with this issue as well

Minimum requirements to plug into state network

- Agencies manage their own resources but at some point we are all interconnected onto the state network
- Everyone that is a part of the state network is managing technology and must meet minimum requirements. If we all meet at least the minimum security requirements, it increases the aggregate for every state agency to be secure

- Standard: Antivirus should be updated daily

Question: Should each agency be required to monitor and use an IDS (intrusion detection system)? Will be visiting this question in the future. However, this may depend more upon resources than anything else (financial and staff)

- Greg encouraged staff to take the information that he had sent out via e-mail regarding the minimum requirements to plug into the state network and to look at and get back to him so he can make changes to the document. Recognizing that this policy was created quite some time ago, and things have changed; nevertheless, state CIO will take information, pare it down, incorporate options, changes, etc and then we can discuss at next month's meeting.

Encryption standard and Data Classification

Greg had a long discussion with the TGB and has incorporated their changes into the policy. It is not as stringent as before. The TGB will be asked to approve the modified standards at the December 14 TGB meeting.

- Basic technical standards are the same
- Difference is the initial standard would have required all laptops be encrypted. Discussion from TGB centered on funding
- TGB has requested DAS to seek funding from the legislature for laptop encryption and that the proposed standard be changed to:
 - All laptops with confidential data must be encrypted by August 31, 2007;
 - If funding is provided by the legislature, then all laptops must be encrypted regardless of the data on them by the August 31, 2007
 - Regardless of funding laptops will be required to be encrypted, whether they contain confidential data or not, by August 31, 2008
- A separate proposed standard would require all agencies to minimally classify their data, either confidential or non-confidential
- The draft standard required all removable media be encrypted and only media approved by a department be used; TGB asked that the standard be changed so only removable media with confidential data are encrypted
- Greg will be seeking volunteers to move forward with the minimum business requirements for an encryption RFP
 - Two-factor authentication?
 - Encrypt to pass phrase?
 - Need to put requirement together, submit an RFP to cover, at a minimum 5500 laptops; as well as to allow local government to

use. The more we get to sign-on to this, the better price we will get from the vendor

- Does not appear that every single agency will require an encryption server, which will help with administration. Anticipate needing 6 encryption servers/agencies to provide encryption.
- Every agency is now required to perform vulnerability testing at least once a year. State Information Security Office can assist with this.

Presentation by Bernard Gaumer:

- Nessus.org – is a free tool; best in class with large online support community.
- ISS, which is a pay money product and offers X-force – team of security professionals as direct support.
- There is a difference between full subscription version and the free subscription version
 - Subscription (full version) – is available and had a direct feed to the developers. It has a 0-day response in regard to vulnerabilities, which in essence gives a 7-day-jump on products that are released
- CVE compatible – includes references to CERT
- Plug-in Architecture – each test written as an external plug-in; can add own tests
- There are 13,022 plug-ins in the direct feed; they do get a little bit more for the fee-based product
- NASL – Nessus Alteck scripting language – can be used to write own security tests
- Up-to-date security, vulnerability database; <http://nessus.org/scripts/php>
- Can test multiple hosts simultaneously
- Smart Service Recognition – security checks not dependent on IANA (Internet Assigned Network Authority) standard port numbers.
- Tests cooperation won't perform sublevel tests for service categories that are non-responsive.
- Complete Reports
- Full SSL Support

How can it help agencies?

- Comprehensive vulnerability assessment
- Can use the information for remediation
- Limited Penetration testing – Can aid security administrators in pen testing but is better used as an internal assessment tool.
- Compliance Audits with a direct feed subscription include:
 - Federal Information Security Management (FISMA)
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Information Technology Information Library (ITIL)
 - National Institute of Standards (NIST) configuration guidelines
 - National Security Agency (NSA) configuration guidelines
 - Payment Card Industry (PCI)
 - Sarbanes-Oxley (SOX)

What it can't do?

- Physical Security for a system
- Remove malicious code for systems
- Actively block malicious code on the network (free version)
- Apply system patches

Greg Fay advised that the State Information Security office does have a tool to use with penetration testing

Can use as a test so can identify exploits and vulnerabilities

State Information Security office would like to use tool more so can assist agencies identified their vulnerabilities

First Step for vulnerability testing is to run penetration tool against ITE networks

Currently running tool on DOT

Have run in past and found small risks

Key here is that agencies should not be concerned with finding vulnerabilities but rather be concerned with the remediation steps to correct the problem. This is about good security practices and not any shortfalls by agencies. Takes a different mindset to realize that finding the security problems BEFORE hackers do is a good thing.

MISC

One question brought up from Judicial is the question of routers managed by ICN. Has anyone had a response when running any type of scan (Nmap in particular) that the router has "failed shut"?

IDS – how can we use as an effective tool between ICN and ITE? Can do internally but cannot make ICN and ITE share IDS logs. Lots of agencies do not have a system to monitor IDS like it really should be. ITE has an IDS system. How can we make this process work better? Greg advised that Adam Kaufman is looking at various IDS system products. Open item. (No resolution today).