OARtech
October 11, 2006

Introductions

Some schools are starting to look CALEA to see how it might affect the campus. One school has the dorms connected to a separate commercial ISP.

Did anyone else have problems with Computer Associates problem? The Computer Associates Anti-virus product update damaged some of the OS.

TJ from Oarnet is still trying to meet his customers. Ann Zimmerman, Oarnet, explained that they had a regional meeting with One Community, Cleveland ring. Oarnet is partnering with them. Presentations were made to schools and other entities in the area. They are not connected to NLR (Case Western is, but not One Community), they are also not connected to I2 and are looking to Oarnet to provide that connectivity.

Ohio University
Joshua Thomas

Mr. Thomas gave a presentation on the Ohio University security issues. Details will not be included in the minutes due to the security issues discussed.

Contact information for questions:
Joshua Thomas, Interim CISO
Ohio University
160 W. Union St., Suite 377
Athens, OH 45701
740-597-2974
Thomasj4@ohio.edu

Lunch

Oarnet Updates
Dennis Walsh

Last mile update
Malone, Walsh, and NASA, and OIT SOMACS are installing last mile connections. When these last mile connections are complete, about 33% of Oarnet members will be connected with gigabit connections to TFN.

SOMAC T1 contract was due to expire, but new contract will not be acted on until the new governor is in place. So they are trying to extend the existing contact. They are also looking at including some Ethernet service in the contract.

Board of Regents asked Oarnet to talk to main campuses for using TFN for branch campuses. They will be talking to the campuses in the future.

Backbone update
They will be closing rings 4 and 5 using KDL out of Kentucky and has been delayed due to an AEP asset problem. The AEP fiber may go clear down to West Virginia. They are

also adding another POP in the northwestern part of the state to service Findlay and other schools in that area of the state.

The I1 gateways are currently running at 75% because of the new pricing as schools have increased their bandwidth. Getting connected to West Virginia fiber for transit and peering for content. The peering traffic does not count against transit charges and would allow peering with CityNet. They are also looking at Level3 over NewNet connection (new I2).

Partners for TFN include K-12 ITC sites and are about 50% connected.
CampusEAI to OSTN (Open Student Television Network) - Campus EAI has asked to become an Oarnet member. Campuses and ONN is looking to put sports broadcasts over TFN as an alternative to using statilite communications. They have been working initially with Miami University. The public broadcasting stations have also been coming on line - they currently have 4 of the 9 connected (WVIZ, WBGN...).

New Directions
They are currently looking at interconnecting with MERIT (Michigan's regional network). They are also looking at connecting to the OmniPOP in Chicago which may have several vendors coming in providing a lot of potential for meshing. They have gotten pricing from several vendors and early projection shows Toledo is the best overall economically. They are also looking at new equipment that may be used to provide this connectivity.

Paul Schopis is chairing the NewNet Technical Advisory Committee in the moving from the Quest to Level3. The have met with NLR officials and discussed roles and possible options. It is clear both network are going to be around for a while. They will be competing networks at this point in time due to the very different business models. The current strategy is to engage both networks and get the best offering for Ohio. Ohio will have connectivity to both networks via Cleveland.

General Datacomm and "The State of Security"
Jim Long and Greg Gillette

General Datacomm (GDC) is a company that came out of ATT and has been in the industry a long time. They weren't known for security solutions, but they have been around and working with many security projects. Greg Gillette is manager for the security division.
They've had partnerships with many of the security companies doing the engineering in the background. Saw the growing problem of security as the networks have grown and as more applications have moved to the data networks.

Today will look at 2 different approaches to security:
Desktop/Agent/Server and agent less approach. The first product he'll discuss uses the agent less approach and can look at network behavior and do analysis based on that behavior: Mazu Networks' tool. Does not use just the signature based view, but also looks at network behavior. It provides a core solution for the large scale customers with total network visibility.

The problem that Mazu Networks sees is a lack of real-time visibility that leads to availability and QoS issues. An increasingly porous perimeter leads to costly downtime, and compliance efforts drains the resources and damages reputations. Most solutions available are not in real time. This results in operational issues with internal security, application visibility and compliance. You want to be able to protect the internal security, but you also want to be able to see applications, and to enforce policy, as well be able to provide reports to validate the network.

Network behavior analysis can model planned changes to the network or policies to determine the impact of the changes on the network. The software allows you to see what happens on the network when you make changes to the network and also allow the modeling of those changes.

The Mazu Profile Platforms helps you to understand how assets and applications are being used and provides enterprise-wide visibility and understand if activity represents a threat/risk with rt behavior analysis and usage and access policy monitoring. The control can now leverage the network infrastructure to enforce policy and respond to threats.

How does GDC use these products? They place the sensors that are tapped into backbone equipment such as routers shipped back to the centralized server. The equipment is not used in-line. The transfer is encrypted and can be controlled centrally. He described some examples in using the product for insider breach, worm outbreaks, application rollouts, etc... and how the product could be used to help verifying compliance to policies, etc....

They have another partnership with Citadel Security Software (recently purchased by MacAfee). The compromises (attacks, etc...) are growing daily. The issues leading to compromise include unnecessary services
(20%), Exposed user accounts (9%), Dangerous user behavior (5%),
Configuration flaws,... . The challenges including shifting from documenting policies to enforcing policies (best practices). The majority of the problems are caused by unsecured accounts, unnecessary services, backdoors, mis-configurations, and software defects or missing patches. You have the control over automating the corrections to these issues.

There are 3 approaches used to define the policies: top-down to check compliance or enforce policy, bottom-up to scan validate and remediate the network, and targeted for near day mitigation. Citadel is a signature based system and thus is near day, GDC provides the automatic implementation of the policy with their product ("Hercules"?).

The security knowledge team that gathers the information, they research the vulnerabilities and possible solutions and design and develop remediation. The quality assurance team tests all the remedies before making them available to customers. Uses Citadel's V-Flash server and then sends to remedy Hercules Server at the client's site. They backup the fix and guarantee the patches.

They provide a solution that may include multiple products that they have partnered with to implement with a specific solution for whatever problems were found.

Meeting adjourned at 2:15 pm