CITOC

COURT INFORMATION TECHNOLOGY OFFICERS CONSORTIUM

Network Security

Technology Experience Bulletin, TEB: 2012-03

Network Security

The California Administrative Office of the Courts was tasked with developing network security standards which could be broadly applied and implemented by the Judicial Branch. These standards were intended to both: assist the local courts in meeting their security needs; and, provide a secure backbone for state-wide initiatives.

Court Context

The Administrative Office of the Courts, or AOC, carries out the Judicial Council of California's official actions under the supervision of the Administrative Director of the Courts. The AOC and the office of the Administrative Director of the Courts were established in 1962 pursuant to a 1960 constitutional amendment.

Tips for Implementation

1. **Consolidate and minimize the ingress/egress control points of your network.**
2. **Do not allow network devices to run parallel to the firewall.**
3. **Limit the access and management of those control points.**
4. **Do not allow direct inbound/outbound network access.**
5. **Limit the ports required for access.**
6. **Apply security patches to all network devices on a routine basis.**
7. **Actively monitor your control points 24/7.**
8. **Keep networks logs in a separate location for at least 6 months.**
9. **Include network security operations in your base budget.**
10. **Policy, policy, policy.**
11. **Document the network.**

Tip 1: Consolidate and minimize the ingress/egress control points of your network. Too many organizations have multiple control points in and out of the network - some dedicated for single purposes. While this may seem to simplify your topology and configuration, it greatly increases the number of exploitation points into the network. You may eventually forget about the small router in some closet that allows access to an entire unsecure partner network. Additionally, while most organizations understand the need to secure access to/from the Internet, they will grant their business partners a less restrictive access point into the network. You must treat all external parties the same – as untrusted entities. You have no insight or control of their network; therefore you must enforce the same security measures. This protects all parties from potential security breaches and liability.

Tip 2: Do not allow network devices to run parallel to the firewall. The firewall must be the one and only control point of the network where all network traffic traverses. If you deploy additional security devices such a web security proxies or VPN devices, deploy them behind the firewall preferably in a DMZ. A parallel architecture negates all the efforts of deploying firewalls in the first place.

Tip 3: Limit the access and management of those control points. Give access to only those responsible for the management and maintenance of the network devices. Avoid having only one person with access and always use unique named user accounts – never share credentials. Also, always require strong passwords that must be changed on a regular basis. Network devices that are directly exposed to outside networks should limit their management access to internal secure networks only.

Tip 4: Do not allow direct inbound/outbound network access. Secure all inbound traffic with a security device such as reverse proxy or VPN, and authenticate your users whenever possible with unique named user credentials that are not shared. This is especially true for vendors and business partners. We tend to issue one set of credentials per vendor / partner, however if those credentials are compromised, you would never know who or how. Servers accessible from outside networks such as web portals, e-mail gateways, etc. should always be place in a DMZ and never inside your secure network. Outbound traffic should also be monitored and managed if possible with web security devices. It is equally important to understand what traffic is leaving your network.

Tip 5: Limit the ports required for access. Open only those ports required for access. Do not cheat for server-to-server connectivity by limiting access using IP addresses. You want to minimize your systems' exposure to any potential vulnerability in the event of any security breach. While ICMP is a popular trouble-shooting tool, do not expose your secure networks using ICMP to any outside network. Audit your control points by scheduling a routine port scan of your perimeter networks to ensure you are only exposing what you intend to.

Tip 6: Apply security patches to all network devices on a routine basis. Organizations now apply security patches and updates to their server infrastructure and end-user devices. However, many fail to stay up-to-date with their network devices. The old philosophy was to leave your network operating systems alone if the network is working fine. If you have an old OS, then you cannot be exposed to new vulnerabilities. In fact, your risk is the exact opposite. Many hackers target old operating systems in hopes that the devices have never been patched. The easiest solution is to subscribe to the manufacturers or 3rd party alert services and create a routine process for the management of network device configuration and patch updates.

Tip 7: Actively monitor your control points 24/7. The deployment of an intrusion detection/prevention system is a critical piece of a complete network security posture allowing you to have an in depth view of all traffic. Subscribing to a security monitoring service is even more important. Most organizations do not have adequate staff to actively monitor and react to real-time threats. Relying on e-mail and SMS alerts for a reaction to any potential intrusion hours later is too late in most cases.

Tip 8: Keep networks logs in a separate location for at least 6 months. You may never need to revert to logs for anything other than trouble-shooting. However, keeping logs for long as possible is critical to identifying a security breach and origination point after the fact. Unfortunately, many sophisticated breaches are discovered too late. The existence of network logs helps the forensics team bridge that gap.

Tip 9: Include network security operations in your base budget. Don't just install the technology – create a budget plan to manage, monitor, maintain, and refresh the technology. No network is secure regardless of the technology if you fail to actively operate and refresh the equipment. It would be a waste of capital to invest in robust, secure network architecture only to allow it to become outdated within a short time of its deployment.

Tip 10: Policy, policy, policy.

The bedrock of strong security is the linkage back to policy. Getting the policy makers involved early to set direction and goals avoids adhoc decision making during implementation. Every situation cannot be foreseen, but having a solid policy base provides both immediate guidance, and a formal process for exceptions and changes.

Tip 11: Document the network.

Full documentation of the network is invaluable in planning the security implementation, making changes, and responding to any issues that may arise. The next team to work on the network will thank you.

Summary

The California Administrative Office of the Courts sought to provide a network security framework to aid local courts and provide secure a backbone for state-wide projects. The development of network policy and guidelines has allowed us to meet these goals.

Author: Raul Ortega, IS Supervising Analyst, Information Security Officer
Network Infrastructure and Security Architecture, Information Services Division, California Administrative Office of the Courts, Raul.Ortega@jud.ca.gov, 415.865.4026

Disclaimer: The advice and opinions represented in this bulletin are based on the experiences of the California Administrative Office of Courts. Such recommendations may not be suitable for other jurisdictions, and are only offered in the spirit of sharing experience as information to others considering the installation of similar technologies.

Approved by the CITOC Editorial Board on December 3, 2012