Outdoor Advertising Association of America

Digital Signage Security Guidelines

Nature of threats

Denial of service – An attacker does not need to gain control of your systems to do damage. They only need to disrupt normal operations.

Unauthorized access – If an attacker gains control of a system they can display whatever they want.

Destructive acts – Any teenager can hack into Google, and learn how play havoc with elevators, mobile phones, garage door openers, and almost any other everyday device…

Areas of concern

Application security – Run applications with the minimum amount of privileges required. Disable or remove any Easter Eggs, or maintenance backdoors. Test for overflow and injection vulnerabilities.

System security – Most systems out of the box are not secure. You will need to perform a full review of services, accounts, and software. Remove or disable what is not needed.

Network Security – All communications should be encrypted by default. Certificates or keys must be used. Each mode of communication has it's own unique exposures whether it is wireless, DSL, Cable or plain old telephone service.

Physical Security – Lockdown and enclose each component. A lock is only a deterrent. Assume that it will be by passed. Cases should have no external screws, route all cables internally. Expose only what you must (antenna's, touch screens,…) Develop automatic fallbacks if any item is compromised. A disabled system is better than a compromised system.

Organizational Security – Social Engineering is one of the most powerful tools available to a hacker. Put polices in place that ensure that information is only revealed to those who need to know, and only through proper channels. Make sure that staff is trained in the policies, and that training is a continuous process. Strategies for protection Defense in depth – Make security an integral part of your Digital signage plans from the ground up. Don't rely on a single piece of software or hardware for security. Assume each device is vulnerable to attack. Just because you have a VPN does not mean your network is secure. Disable unused ports on your Ethernet switch. Disallow all network cards, except for the MAC addresses you know should be on your network.

Keep it simple – Reduce the avenues of attack by removing all applications and services that are not needed.

Locked down by default – remove or disable all guest or system accounts that are not needed. Use strong passwords, change them periodically, and do not have one universal password that gives away the keys to the kingdom if compromised. Remove the easy web configuration software on your router.

Keep it current – Prepare a plan for patch management. Ensure you identify all items that could need security patches or firmware updates. Routers, hubs, touch screens. Every day hackers find new ways to wreak havoc. Security must a be 7x24 task.

Get Audited – Bring an outside expert to review your signage design.

Involve Everyone – Make sure that staff is trained in basic policies, and procedures. Only share information with known people outside the company.

Watch it closely – Turn on logging and enable monitoring of each system that you can, and prepare for off hour notifications via e-mail or pagers. The dead of night and holidays is primetime for hackers.

Know your enemy – If Hackers have a weakness it is their need for attention. Exploit that. They post their conquests online for you to learn from. Simple Google searches with the words hack crack phreak…combined with any of your particular hardware or software components will reveal what you will have to protect against at a MINUMUM!

For further Information

http://www.us-cert.gov/cas/alerts/

http://sectools.org/

http://www.networksecuritytoolkit.org

Hackproof your network
http://www.elib.hbi.ir/computer/networking/pdf/%5B1928994156%5DSyngress%20-%20Hack%20Proofing%20your%20Network%20Internet%20Tradecraft.pdf