Outdoor Advertising Association of America

Digital Billboard Security Guidelines

Introduction

Digital billboards are strategically placed to provide great visibility in high traffic areas. A successful cyber-vandalism attack against a digital billboard will be very apparent and will have a financial impact to operators or agencies who own any attacked billboard.

Hacking incidents also generate unflattering publicity. In the past, reporters have pursued billboard operators for on-air explanations of the problem.

What Can I Do?

To protect against losing control to an outside hacker:

Improve Password Strength

Do not rely on default passwords from display manufacturers. Do not use common passwords for multiple displays.

Use at least eight characters and change passwords every three months. When creating passwords, do not use dictionary words or terms associated with you. Instead, try creating a password using the first letter of each word from a phrase you can remember and add punctuation. For example, the strong password “Mhall;ifwwas!” could be remembered by recalling the start of the children’s story “Mary had a little lamb; its fleece was white as snow!”. Further strengthen the password by using capital letters, numbers, and symbols where possible: “Mh@LL;ifWWa5!”

Implement Whitelist Access

Only allow you or your company’s IP address to reach the management services on your billboards.

Use Multi-factor Authentication

Check with your billboard vendor for solutions that require a token, key fob, or other authentication method instead of relying solely on pass words.

Use a VPN

Virtual Private Network (VPN) use protects the billboard against access both by normally requiring strict authentication methods and by encrypting traffic in transit between you and your billboard.

Apply Security Patches

Software vendors produce security patches and software updates as new vulnerabilities are discovered, and normally make them available on web sites. Billboard administrators should apply these security patches as soon as they are made available to ensure their billboards are as secure as possible.

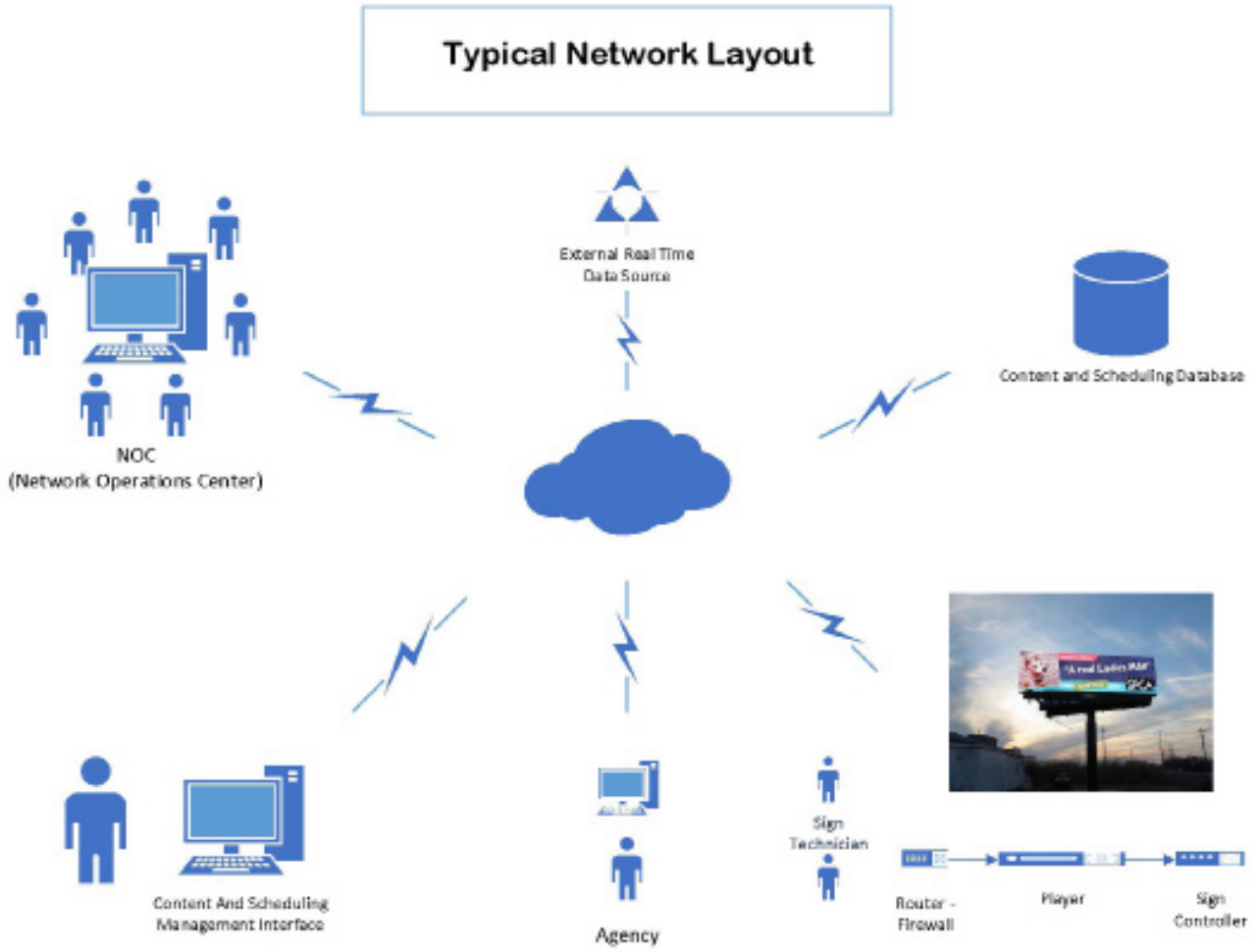
Disable Unused Services

Billboards can have many different ways to manage their configuration and content. Turn off any management methods which are not used to reduce the potential for a hacker to access the billboard.

To protect against losing control to an inside individual (in addition to the steps above):

Trust, But Verify

Just as you would conduct a background check on a potential employee, any individual who you trust to have access to your billboards should be verified to be trustworthy.



Appoint a Security Officer

A single individual (or small team) should be responsible for managing employee access to billboards. Employees who depart or no longer require access due to position should have access to the billboards removed.

Consider Third-party Security Tools

External vendors can provide security-related recommendations and services to ensure the security of your billboards. Some of these services could include Virtual Private Networks, Intrusion Detection Systems, Vulnerability Scans, Managed Firewalls, Multi-factor Authenti cation, and Patch Management.

To protect against losing control to a physical security breach:

Install Security Devices — Fencing, door alarms, and trespass cameras all provide deterrents to physical access, but these should also allow for an automatic response. If any unauthorized access is detected, the billboard's ad rotation should be interrupted.

Install Remote Interrupts — In an undesired scenario where someone has gained control of your billboard, remote power interrupts or other methods to shut down your billboard would be beneficial.

After The Hack

The following "to-do" list will prepare you for an appropriate response should one or more billboards fall prey to an external, internal, or physical breach:

- Activate an Emergency Response Team consisting of (at a minimum) Legal, Information Technology, Public Relations Officer, and Management personnel.
- Notify Law Enforcement – know who to contact at any time of the day or night.
- Prepare for the press and media attention.
- Take steps to prevent more incidents.

EXPERT TIP

Establish relationships with law enforcement agencies and vendor support before you need to reach out after a hacking incident.

How Do I Start?

- Conduct a self-examination using the recommendations above to gauge your current security posture.
- Identify which security improvements can be made with the least effort and begin the implementation process with these.
- When a road block is reached or for guidance specific to your billboard, contact your billboard vendor's customer service security person.

For More Information

For more information about preventing billboard hacks, how to get law enforcement involved, or to contact a digital billboard provider in the United States, please contact OAAA at (202) 833-5566 or info@oaaa.org.

Glossary

Intrusion Detection System (IDS): An IDS will monitor computer network communications to identify potentially malicious traffic. The actions taken by an IDS could be to simply alert security personnel to the communications or to block the communications to protect the billboard.

Multi-factor Authentication: The use of two or more disparate methods of determining access privileges. This authentication method typically uses the categories of something you know, something you have, and something you are. Some current implementations include the use of a password with one of the following second methods: a hardware token generator, a service that sends a code to your mobile phone, or a biometric device to read fingerprints.

Patch Management: A process (manual or automated) to apply security updates to services and systems as they are released by vendors.

Virtual Private Network (VPN): A VPN is either a program or a physical device that connects to a remote endpoint to connect two networks securely. The link between both endpoints of a VPN should be encrypted, and the endpoint programs or devices should have a method to positively validate the identity of the opposing endpoint.

Vulnerability Scans: Vulnerability scans are automated queries of systems and services used to identify weaknesses which can be exploited to provide attack vectors to hackers.

Whitelist: In the realm of network access control, a whitelist prohibits access to a service or system from unauthorized sources. For example, a whitelist on a digital billboard's management service could be configured to allow access from only its operator's computer network. This method of restriction significantly mitigates the risk of an external hacker attacking the billboard.