Official Knowledge Session Handout of:
MICHIGAN REALTORS®
THE CONVENTION
Amway Grand Plaza Hotel & DeVos Place, Grand Rapids • Sept 27-29, 2017

SUN TITLE

Data Security Best Practice Tips

Data security encompasses a wide variety of practices, methods, and procedures based on the type of organization, technology topology, and type of data being protected. While not all of these combinations can be accounted for in a single document, there are general concepts that can help direct the planning process for any organization. These practices can be divided in terms of Hardware, Software, People, and Processes. Below are a list of items that can be dissected and expanded upon in order to help provide a more comprehensive plan tailored to specific needs.

Hardware

Perimeter:

- Higher end firewalls, such as Cisco and Watchguard allow for advanced security features including:
  - Web content filtering.
  - Anti-virus scanning.
  - Reputation, application, and protocol protection.
  - Advanced threat protection for Zero-Day exploits.
  - Data loss prevention and auditing policies.
  - Deep Packet Inspection of HTTPS traffic.
  - Geolocation-based blocking.

Wireless Security:

- Identity-based 802.1x authentication.
- Wireless Intrusion Prevention.
- Properly separated guest, employee and production networks.

Systems Monitoring, alerting, and log collection:

- Collection of logs at every critical point in the network, including firewall/router and front-end and back-end systems.
- Security monitoring and alerting based on smart triggers.

Infrastructure:

- Redundant, robust, and encrypted backup strategy using the 3-2-1 rule.

Mobile:

- Institute a Mobile Device Management (MDM) system to manage manage corporate and Bring Your Own Device (BYOD) equipment.

Software

- Enable 2-factor authentication to domain registrar, DNS, and other hosting environments.
- Implement DNSSEC to ensure that DNS records cannot be compromised or taken over.
- DKIM and SPF record to protect against malicious domain spoofing.
- Use industry leading spam and virus filters, like Mimecast, or Proofpoint, to filter and protect against spam, viruses, phishing, and malicious attachments.
- If systems support it, enable email transport encryption.

Infrastructure:

- Regular software and firmware updates to critical components, including servers, workstations, and network infrastructure components.

People

- Train employees to be aware of anything that might look different outside of their normal world. This can include email, phone, other forms of communication, or people without proper identification. Train with real examples to make a strong impact. Red team exercises are also beneficial.
- Never enter login information outside of the normal outlets, especially email.
- Don't open unexpected, unsolicited, or suspicious attachments. Always verify with IT when possible.
- Ensure data is saved to trusted network/server locations and do not allow USB storage devices.
- Instill trust between employees, IT, and security. Employees must understand that their IT departments are there to help. If an employee falls victim to a scam or phishing attack, IT, and security, can provide remediation resources to the individual and organization. Not having this trust in place can only worsen the effects of the attack.
- Conduct unannounced phishing testing on a periodic basis using a trusted, third party firm, like Information Navigators.

Procedure

Access Controls:

- Role-based file permissions.
- File system and application specific permissions.
- Dedicated service accounts to isolate access to critical systems if one is compromised.
- Least privileged database accounts with minimum required access.
- Complex, yet enforceable, user password policies.
- Multi-factor authentication.
- VPN connections for remote users.
- Penetration testing utilizing services like Information Navigators by Dickinson Wright PLLC.

Client and Endpoint Security:

- Software restriction policies.
- Removing administrator permissions from users.
- Regular anti-virus scans and reporting.
- Software patching.

Infrastructure:

- Disaster recovery and incident response planning.
- Emergency preparedness for natural and man made events.

Physical:

- Locked doors with proper access to employee and infrastructure areas.
- Clean desk policies.
- Proper identification for staff and vendors.