LFMA – 2018 – Securing Your Data

Mike Bohlken – Sr Director IT, Lutheran Social Service of MN

The following are highlights from the "Securing Your Data" presentation

- **Check to see if your password has been used in a data breach**
  - https://haveibeenpwned.com/
  - Click Passwords to test if your password has been used in a breach

    RECOMMENDATIONS:
  - Do not use passwords that have been used in past breaches
  - Change your passwords – suggest password phrases
  - Don't use the same password for different accounts
  - Don't write down your passwords, suggest using an application such as LastPass

- **Cloud Services**
  - Microsoft offers discounts to qualified non-profits
  - See details at https://www.microsoft.com/en-us/nonprofits
  - Techsoup also offers generous discounts on software
  - See details at https://www.techsoup.org

    RECOMMENDATIONS:
  - Take advantage of non-profit pricing
  - Microsoft offers Office 365E1 licensing for free – details about this product can be found at https://products.office.com/en-us/business/office-365-enterprise-e1-business-software

KEEPING THE BAD GUYS OUT

Ransomware –is when a hacker maliciously locks the files on your computer. You can pay a fine through bitcoin to unlock your machine

RECOMMENDATIONS:

- Make sure computers are backed up regularly – LSS of MN uses a program called CrashPlan - https://www.crashplan.com
- Computers are locked down so that only the IT department can install programs. This eliminated the ransomware threat

Phishing– is when a hacker tries to trick employees to give up credentials, so they can breach the system. **Spear Phishing** – is when a hacker imitates a person of authority to authorize a fraudulent financial transaction

RECOMMENDATIONS:

- Education – LSS of MN uses a product called KnowBe4 for education and to run phishing simulations. https://www.knowbe4.com/
- Implement 2 factor authentication as part of the Office 365 rollout – prevents hackers from getting in even if the person has been phished
- Branded I.T. – all emails from I.T. will have a branding logo so employees know the email came from IT. Also, IT stopped sending emails from the admin account.

Network Lockdown

RECOMMENDATIONS:

- LSS of MN prevents access to the guest wireless unless an employee allows them access
- Non-LSS devices cannot plug into an ethernet port

Server / Firewall Patches

RECOMMENDATIONS:

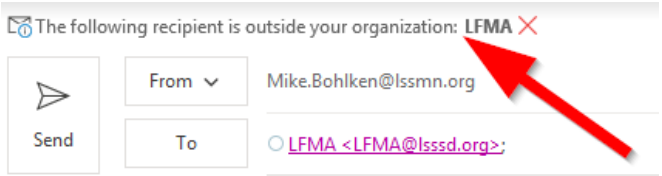
- Microsoft security patches are applied on the servers on a regular basis
- Review what files are on the outward facing servers so that no important data can be stolen

DATA LEAKING

Email – data can leak accidently through email, accidently forward and send to the wrong recipient

RECOMMENDATIONS:

- Exchange server has an option to indicate when an email is being sent outside the organization



- Office 365 showed us who auto-forwarded and email outside the organization

Cell Phone / Tablets – data can leak when email attachments are saved on these devices

RECOMMENDATIONS:

- Implement a product from Microsoft called EMS-E3 (LSS of MN does not currently do this)
- Allows your phone to be containerized so the container can be remotely wiped
- Does not allow company data outside the work container

Shared File Service – shared files services such as dropbox, box, google drive, amazon cloud, etc pose a problem when an employee leaves the organization. Ex-Employee will still have access to those documents and can represent themselves as a current employee.

RECOMMENDATIONS: (LSS of MN is exploring these solutions)

- Implement an enterprise solution so that ex-employees cannot access their files
- Make sure that the product is configured to use a single sign on – which uses the company active directory
- Block non-approved sites

Cloud Software – Due diligence should be taken when considering a SAAS (software as a service) solution

RECOMMENDATIONS:

- Can the vendor supply a SOC2 report – https://www.incapsula.com/web-application-security/soc-2-compliance.html
- Does the application work with your Active Directory (SSO)?
- Does the application user 2 factor authentication?
- Make sure there is a policy about running reports or exporting data on a non-network computer

BEING PROACTIVE

RECOMMENDATIONS:

- LSS of MN hires a dedicated Cyber Security Analyst to focus on security/policy issues
- Education – never enough. Make it fun and offer giveaways to those that do good
- Investigate the many Network tools – they are expensive, but may predict an intrusion
- Microsoft Tool – EMS-E3 provided Mobile Device Management, Advanced Threat Analytics and Data Encryption

OCTOBER IS CYBERSECURITY AWARENESS MONTH!