Privacy, Security & Accessibility Committee
Meeting Minutes
January 15, 2020

PSA Marmot Security Report

The Marmot team shared an analysis of the security measures currently in place across all services: ILS, Pika discovery, staff password protocols, operating system updates and patches, and the network. An outline of this presentation can be accessed here.

ILS - Brandon

Marmot provides an annual audit of Sierra users and logins via Tableau in the yearly clean-up section and they notify members in Spring for review. Marmot also pays attention to staff turnover and will reach out to institutions if they think password changes are necessary. For 3rd party vendors they only use Secure Patron API = HTTPS instead of HTTP for data transfer. Marmot admin passwords are very secure (special characters, upper/lower case, etc.) and passwords are not reused. They also enforce limited permissions so only those who need access to a particular action receive it. Marmot endeavors to stay on the most current release of Sierra.

Discovery - Sean

All traffic on all of the discovery layers is encrypted via HTTPS.

IT - Sean

All web services are also HTTPS. Personally identifiable information though managed services like PC Reservation are purged nightly. Third party vendors like Bibliotheca are given specific accounts to access to the network and this access must be requested.

Physical Security - Sean

To access the Marmot offices they use electronic door locks that are enabled via RFID. Doors are locked at all times so they can monitor who comes and goes in the building. Staff computers are logged off each night and passwords are not available via post-it notes - lots of jokes in chat about using post-it notes.

Strong Passwords - Sean

Use strong/complex passwords and they have an in-house database to track passwords, but they are looking for a more tiered structure. After doing some research they have determined that LastPass is the product they will adopt.

Operating System Patches - Sean

Test systems are patched at the beginning of the month to see if they will break before applying the same patch to production servers. If safe, production servers are patched the following week. Switches and firewalls are patched when a new version is available and computer workstations throughout Marmot are patched on Wednesdays and Sundays.

Network - Sean

Intrusion detection is turned on for the firewall. Marmot had some issues with foreign countries so China and North Korea are blocked, but it turns out that there are legitimate patrons from Russia who are working in the US and use our libraries to access their Russian email, so they have not been blocked. Mamort utilizes multiple content filters to block malicious sites, adware, spyware, etc., from accessing the network: Cisco-Meraki Firewall, Piehole. PRTG (Passler Router Traffic Grapher) is used to monitor updates, traffic loads, temperature/humidity of the server room. Lastly they use an external audit to check for vulnerabilities and holes.

Question on External Audits - Sean & JB

How are they conducted - do we pay someone for this service? Ans: You can pay an agency to do a scan and give you a report - these are very good. There are ways for Marmot to do some of this themselves. Marmot will be implementing both approaches.

Is this vulnerability or penetration testing? Ans: Marmot does mostly vulnerability. Some penetration testing is done by scanning for open ports and services, but not they do not employ a white hat hacker. When vulnerabilities are disclosed by the testing, Marmot examines their systems/network to make sure any necessary patches have been implemented. Outside agencies cannot see patches, they can only detect the major version numbers of the operating systems in use.

Discussion on Password Security

Paul, Montrose Public Library, uses KeyPass as does Marmot. KeyPass is a reasonable option for a small organization within a single building. Sean discussed again how Marmot was getting ready to implement LastPass due to a number of advantages: able to access outside of the office, cloud based, tiers of permissions.

Alysa, Bud Werner Memorial Library, uses LastPass. Originally all of their passwords were stored on their Intranet. All managers are encouraged to change their master passphrase annually. Work hard to not reuse passwords and they share logins/passwords via a shared folder system on LastPass. They also encourage staff to have their own LastPass account which can be linked to their corporate account. This way private passwords are saved to the personal version while still using the corporate. LastPass also comes with an app.

Shauna, Mesa County Public Library, does not have a password manager but they do have a policy that all employees are expected to sign. With 100 employees LastPass would be challenging to implement. They try to limit the number of accounts that staff can access and supervisors keep track of which accounts their employees have access. When a staff member leaves the login information gets changed or they do it every 6 months if there is no turnover. Try not to have too many generic passwords so staff all have their own windows and Sierra accounts. They require the use of strong passwords that are not reused.

Bemis is under the umbrella of the City and must follow their policies. Have a few shared logins for Sierra both for the desk and volunteers in Tech Services. They change their City passwords every three months. It's a balance between convenience and security.

Shane uses LastPass and the desks use the same Sierra login throughout the day.

Nicole does not use a password manager but like Shane, if a student/staff member leaves they will update the shared login at the end of the semester.

Alysa does the same - sharing one Sierra login for desk staff throughout the day. She admits that they have not been changing shared Sierra logins with turnover.

Size of the institution really dictates what can be reasonably implemented.

Niclole asked Marmot if they had any recommendations/best practices/comments regarding password managers. Sean encourages the use of a password manager. Brandon addressed the shared nature of Sierra logins and talked about the password manager options within this platform. Sierra logins can be set to expire at a specific time forcing staff to update their passwords. Brandon also felt that this group would be the one to come up with best practices/recommendations for all of Marmot. Sean remarked that good security is not about convenience - we have to come up with systems that make it as painless as possible. Brandon also said they can limit access to Sierra to a range of IPs, this would keep old staff from accessing it outside of the building. This limit would be applied to all accounts, you could not limit it to just some. Where this could be an issue is for a Bookmobile that uses wifi for access. Anyone who would want to log into Sierra from home would be encouraged to use a Marmot VPN (Virtual Private Network) if IP restrictions were in place.

Nicole suggests we make it a task of the committee to develop best practices/policy regarding password management. Shauna feels it is very important and sees this committee coming up with a number of issues that we will want to recommend to be implemented as a best practice, policy, etc. so there should be a mechanism where we make recommendations to the Marmot Board, directors - or are we empowered to just make policy? Other members felt that it would be useful if we had official direction.

What do we want to work on?

Last Meeting Ideas - audits for data, vendor privacy policies (Nicole could do a mini-training on vendors)
Sean - password policies covers the concerns Marmot has for the consortium, suggests that Marmot outlines the holes and issues that they see need strengthening (e.g., lack of pin or passwords for patron accounts.
Alysa - wants to understand GDPR, CA & CO laws and the request for personal data. What do we store and how would we supply this to a patron if asked. We should also offer training on how to handle these requests.
Nicole - After auditing our data we should create a privacy policy and share what is being collected publicly - both internally and via vendors.

Next Meeting?

Nicole suggests a monthly meeting as opposed to every other month. Everyone agreed that monthly would be best. We'll be sticking to 1 hour. Nicole will send out a Doodle Poll for the next meeting time

As to the topic for the next meeting, Nicole will start a spreadsheet and we are encouraged to add to this sheet.

Library Freedom Institute (LFI) - shared by Nicole via email

As I mentioned yesterday, I wanted to let everyone know that there is a new cohort starting in March 2020. LFI is free of cost, a five-hour commitment per week (including 1-2 hours in real time), and mostly online with one in-person weekend component. The next 2 cohorts will be 4 months long (and both will be in the next calendar year, I believe). Pending funding for LFI, the goal after that is not to have more cohorts after that but to continue building the team from all previous cohorts, so I'd encourage everyone to take advantage of the institute now. I would also highly recommend this institute. For me it was very transformative. The cohorts that graduated have formed one group, and we are very active. You can find more information, and the application, on the website: https://libraryfreedom.org/index.php/lfi/