Open the Gate! Ensuring Easy Authentication While Mitigating Cybersecurity Risks

John Felts
Presenter

David W. Green
Presenter

Matthew Ragucci
Presenter

Todd Enoch
Recorder

Abstract

The ability to work remotely has been a blessing in some ways, however, library users still face challenges. To compound matters, cybercrime risks loom large threatening campus security, specifically targeting users who are accessing resources remotely. This has uncovered skills gaps for both librarians and users, requiring librarians to examine their authentication methods. Thankfully, there are easy ways to ensure institutional security, while also reducing barriers to paywalled content for users. Reporting from both the librarian and publisher perspectives, this paper provides insight into remote authentication challenges, library cybersecurity risks, and solutions for protecting institutions while still providing seamless access.

Keywords: authentication, e-resources, cybersecurity

This session was designed as a panel presentation on protecting libraries from increasing threats of cybercrime with librarians and a vendor discussing practical strategies and best practices.

Matthew Ragucci started off the session speaking about the propensity for hackers to target higher education for cybercrime, attributing it to several factors. First, a university's high population number provides a larger pool of people for the hackers to target with their phishing e-mails. Second, a university's information on past and current students, faculty, and vendors is valuable to cybercriminals. Third, valuable research, particularly from engineering and medical fields, serves as a target for espionage. Finally, the fast pace of research pressures universities into fast, expensive solutions. It is estimated that 75 percent of higher education cyberattacks succeed.

To give some context to the risks cybercrime pose to academic institutions, Ragucci provided some data from the National Cyber Security Center (NSCC) website.[1] In August 2018, researchers found over 300 fake websites and login pages linked to seventy-six library systems around the world. The United Kingdom's National Cyber Security Centre lists the education sector as the third largest target for cybercrime, ahead of retail. And a leading medical-research institution working on a cure for COVID-19 had to pay $1.14 million to recover control when its servers were hacked in a ransomware attack.

Next, John Felts spoke from the university librarian's perspective. He mentioned that while people often hear about the attacks on larger research universities, there are probably many more attacks on smaller institutions that go unreported. He described a recent attack on a small college with under 500 full time equivalency where the invasive software had been lying in wait in the servers for months before being activated the day before finals week began, taking control of everything including the institution's emergency broadcast system which the hackers used to broadcast messages across campus until the hackers were paid.

Libraries are especially vulnerable to cyberattacks because they are seen as a potential backdoor to the data housed by the institution due

to the high volume of traffic through the library website. Librarians have an ethical responsibility to protect the data that can be accessed via stolen credentials, such as patron information (email accounts, financial information, address, and phone number); institution assets (research and budgets); and publisher assets (licensed and proprietary content). They are also well-positioned to serve as security advocates, a role which aligns well with their role as privacy advocates. Compared to other university departments, libraries are unique in the types of information they host and provide access to in both relationships and content. While libraries may often defer to campus Information Technology (IT) departments on both privacy and security topics, it is incumbent upon the library to be cognizant of user privacy and data security.

Felts related an anecdote about the effectiveness of two-factor authentication in reducing the effectiveness of phishing attacks, as the authentication software provided an alert that the password was compromised and prevented the hackers from accessing the system while also allowing time for the compromised password to be reset. He stressed that educating users about two-factor authentication and encouraging its implementation can go a long way toward mitigating risks and protecting patrons.

Another area of concern for cybersecurity is Internet Protocol (IP) Authentication. There is a perception that IP authentication is more privacy-preserving than federated authentication, but that is not necessarily the case. IP addresses can identify individuals who have a dedicated IP address. Additionally, when institutions use proxy servers that include some type of uniform resource locator (URL) rewriting method, such as EZproxy or Web Access Management (WAM), this leaves them vulnerable to IP spoofing, man-in-the-middle attacks, clickjacking, and session hijacking. Blocking IP addresses as a security measure is a blunt tool: if a vendor identifies one compromised user account using the proxy IP, access could be cut off for the entire institution instead of for an individual account. Identifying and isolating the compromised or malicious user account can be more easily resolved with federated

access. One issue to be aware of is a coming change in how Internet browsers handle cross-platform cookies which could negatively affect the ways that libraries handle authentication.

The preferred alternative to IP filtering is federated identity management, which utilizes a more reliable, robust, Security Assertion Markup Language (SAML)-based infrastructure. Compared to IP filtering, federated access is typically easier to maintain, supports multiple user affiliations, and provides a better user experience. Felts described the spike in authenticated sessions at his library following the implementation of federated access even before they had updated their institution's URLs.

Next, the presenters played a pre-recorded segment from David W. Green about efforts at the State Library of Ohio to address cybersecurity. Green first discussed the shared responsibility model of cybersecurity wherein both the user and provider have obligations to maintain security. He highly encouraged people to seek out conferences, workshops, and newsletters on cybersecurity to stay up to date on best practices and new issues. He also stressed the importance of collaborating with local IT departments.

Because the library is perceived as a learning hub for the community, librarians can take advantage of that to help promote cybersecurity to both their colleagues and patrons. For example, during COVID-19-related library shutdowns, the State Library of Ohio held virtual office hours to assist patrons and used those times to promote cybersecurity awareness. They also participate in Cybersecurity Awareness Month and are working on expanding their awareness activities to be a regular activity throughout the year. Some institutions have cybersecurity briefings breaking down recent issues, which can be a helpful tool in learning how to avoid or address these problems.

It is important to implement established security practices such as better password management. Utilizing a password manager to maintain passwords helps users meet the criteria for unique and complex passwords rather than relying less secure methods such as writing them on post-it notes or entering them in spreadsheets. You may also

conduct a password analysis to ensure you are not reusing passwords across multiple sites.

Other established security practices include installing secure sockets layer (SSL) certificates on all websites, frequent backups to lessen the danger of ransomware, and, when possible, moving to cloud-based services to reduce the amount of security maintained on site. It also is important to have a plan in place for how to deal with cybersecurity threats; even if the institution has a plan in place, it is nonetheless important for the library to have a plan to address library-specific issues.

Finally, Ragucci offered a vendor's perspective on cybersecurity. He stressed that security is a multi-stakeholder concern, affecting both users and providers. Cybersecurity is about striking a balance and finding a way to grant users access while also maintaining privacy and protection. Publishers have robust abuse monitoring systems which are intended to not only protect the vendors' content, but also to protect the institutions and their users who may not realize they have been compromised.

Some ways in which comprised accounts can affect institutions include disruptive IP blocks which shut off access; ransomware attacks; and inflated usage which can affect collection development decisions. Some potential solutions include SAML-based authentication; EZproxy's Pseudonymous Identifier which can keep the disruptive IP block from happening by associating the use with a single user rather than the proxy IP; and publisher-led friction reduction initiatives such as GetFTR, Seamless Access, and Content Syndication.

Ragucci ended the presentation by discussing the Scholarly Networks Security Initiative (SNSI), a group that brings together publishers and institutions to solve cyber-challenges threatening the integrity of the scientific record, scholarly systems, and the safety of personal data. Members include large and small publishers, learned societies, university presses, libraries, and others involved in scholarly communications. SNSI has developed tips for academic librarians on building strong information security defenses at their institutions, many of

which were discussed over the course of the presentation, but which can be summarized into two types of actions: first, to develop, investigate, and share knowledge about cybersecurity and second, to implement that knowledge in day-to-day practices.

Contributer Notes

John Felts is Head of Information Technology and Collections, Coastal Carolina University, Conway, South Carolina.

David W. Green is Library Systems Analyst, State Library of Ohio, Columbus, Ohio

Matthew Ragucci is Director of B2B Product Marketing, Wiley.

Todd Enoch is Head of Subscription and Resource Management, University of North Texas Libraries, Denton, Texas

Note

1 National Cyber Security Centre, *The Cyber Threat to Universities* (National Cyber Security Centre, September 2019), accessed December 15, 2023, https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities.