Empfehlungen zu IT-Sicherheit in Bibliotheken

Ein Arbeitspapier der Facharbeitsgruppe Technische Infrastruktur (FAG TI) im Gemeinsamen Bibliotheksverbund.

Version 1.0 vom 23.8.2024

Die FAG TI beschäftigt sich konstant mit IT Infrastruktur in Bibliotheken und deren Absicherung. Dieses Papier richtet sich sowohl an Bibliotheksmitarbeitende als auch an IT-Verantwortliche und die Empfehlungen beginnen mit allgemeinen Hinweisen und enden mit eher an Technikverantwortliche gerichteten Aspekten. Mit der sich verändernden Bedrohungslage werden sich auch die Empfehlungen verändern, daher handelt es sich hier um eine Momentaufnahme.

Regelmäßige Sicherheitsschulungen für Mitarbeitende

Schulungen sind essenziell, um den sicheren Umgang mit IT-Systemen und Daten zu gewährleisten. Durch kontinuierliche Schulungen bleibt das Personal auf dem neuesten Stand hinsichtlich aktueller Bedrohungen und Schutzmaßnahmen. Dies minimiert das Risiko menschlicher Fehler, die oft Einfallstore für Cyberangriffe sind. Nur durch fortlaufende Weiterbildung kann sichergestellt werden, dass Sicherheitsrichtlinien effektiv umgesetzt und Sicherheitslücken rechtzeitig erkannt werden. Neue Mitarbeitende sollten sofort im Rahmen des Onboardings in grundlegende Sicherheitspraktiken eingeführt werden, bevor sie Zugang zu IT-Systemen erhalten.

Informationsseite zum Social Engineering: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html
3-Sekunden-Sicherheits-Check: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/E-Mail-Sicherheit/e-mail-sicherheit_node.html

Passwortmanager

Für einen sicheren Umgang mit Logins (Kombination aus Loginname bzw. Emailadresse und Passwort) ist es notwendig, Passwörter nicht mehrfach zu verwenden. Wenn ein Passwort in falsche Hände gerät ist sonst nicht nur der betroffene Service gefährdet, sondern alle Services, bei denen das gestohlene Passwort genutzt wurde. Diese Anforderung führt jedoch in Kombination mit der Notwendigkeit, lange und komplexe Passwörter zu verwenden oft dazu, dass sich Menschen die häufig zahlreichen Logins nicht mehr merken können. Aus diesem Grund existieren so genannte Passwortmanager.

Passwortmanager dienen der sicheren Speicherung von Logins und bieten darüber hinaus i.d.R. noch weitere Komfortfunktionen an. So können die meisten Passwortmanager sichere Passwörter nach Zufallsprinzipien erzeugen. Browser-Plugins oder copy-paste-Funktionen erlauben das (halb-)automatische Ausfüllen von Passwortdialogen, so dass kein Abtippen der

Passwörter mehr nötig ist. Passwortmanager erlauben es auch, einen Überblick über alle Logins zu behalten, so dass man sich zum Beispiel bei nicht mehr benutzen Services löschen lassen kann.

Passwortmanager gibt es als Cloudlösungen, als kommerzielle Software und als Open Source-Software. Im kostenfreien Open Source-Bereich sind unter anderem KeePass2 (https://keepass.info) und KeePassXC (https://keepassxc.org/) erprobte Optionen. Diese legen eine verschlüsselte Datei an, in der dann die Logins sicher gespeichert werden.

Der Umgang mit Passwortmanagern sollte im beruflichen Kontext geschult werden, da Passwortmanager bei falscher Anwendung ein Sicherheitsrisiko darstellen können. Dies hat dann im schlimmsten Fall den Effekt, dass alle im Passwortmanager gespeicherten Logins Angreifern zur Verfügung gestellt werden, was unbedingt zu verhindern ist. Hier ein paar Punkte zum sicheren Umgang mit Passwortmanagern:

- Fremdgehostete Cloud-Lösungen sind generell nicht zu empfehlen, da die Passwörter (wenn auch verschlüsselt) regelmäßig über das Netz übertragen werden und man als Kunde keinen Eindruck davon bekommt, wie sicher der Dienst mit den Passwörtern umgeht. So wurde z. B. der Passwortmanager LastPass im Jahr 2022 gehackt. Die Logins wurden bei LastPass zwar verschlüsselt gespeichert, aber die Angreifer konnten mit so genannten Brute Force-Angriffen versuchen, diese zu entschlüsseln, was bei der Verwendung unsicherer Master-Passwörter (s.u.) schnell gelingt.
- Passwortmanager wie KeePass2 und KeePassXC speichern die Logins in einer verschlüsselten Datei, die lokal gespeichert wird. Eine Beschädigung oder versehentliches Löschen der Datei führt im schlimmsten Fall zum Verlust aller Logins. Daher sollte die Datei gut gesichert werden (Backups) und/oder es sollten zum Beispiel auf Papier ausgedruckte Kopien der Logins an einem sicheren Ort verwahrt werden.
- Die Sicherheit von Passwortmanagern steht und fällt mit der Sicherheit des Master-Passworts, mit dem man Zugriff auf die abgelegten Daten erhält. Ein unsicheres Master-Passwort führt schlimmstenfalls dazu, dass alle Logins in die Hände von Angreifern fallen, was katastrophale Auswirkungen haben kann. Somit müssen unbedingt von allen Nutzer*innen sichere Master-Passwörter vergeben werden.
- Bei der Auswahl eines Passwortmanagers sollte natürlich ein sicheres Produkt verwendet werden. Sicherheitsprüfungen (Audits) durch unabhängige Institutionen sind ein guter Hinweis auf eine sichere Software. Die Hersteller weisen üblicherweise auf den Produktwebseiten auf erfolgreiche Audits hin.
- Passwortmanager sollten regelmäßig auf Updates überprüft und aktualisiert werden.

Bitte beachten Sie auch: Verschiedene Browser erlauben die Speicherung von Logins ohne zusätzliche Software. Dies ist aber i.d.R. unsicher, da Browser angreifbar sind und die Logins oft nicht verschlüsselt abgelegt werden. Auf die Speicherung von Logins in Browsern sollte unbedingt verzichtet werden. Weiterhin sind Browserplugins lokal installierter Passwortmanager zwar sicherer als die Speicherung von Passwörtern im Browser, aber aufgrund der o.g. Angreifbarkeit von Browsern ggf. auch nicht sehr sicher.

Bei korrekter Verwendung können Passwortmanager in hohem Maß zu dem sicheren Umgang mit Logins beitragen. Dafür ist aber wie beschrieben ein verantwortungsvoller Umgang mit Passwortmanagern nötig.

Umgang mit Nutzer-USB-Sticks

Ein grundsätzliches Problem stellen mitgebrachte USB-Sticks dar. In Auskunftssituationen wünschen Nutzer*innen gelegentlich, dass die Kolleg*innen einen Blick auf die Inhalte des USB-Sticks werfen, zum Beispiel um Literaturlisten zu prüfen oder um in darauf gespeicherten E-Medien zu recherchieren. Leider ist die USB-Schnittstelle ein mögliches Einfallstor für Schadsoftware - so können sich Schadprogramme, die auf dem USB-Stick installiert sind, zum Beispiel als angeschlossene Tastatur ausgeben und auf diese Weise Zugriff auf den Rechner erhalten. Aus diesem Grund sollten fremde USB-Medien nur an Geräte angeschlossen werden, die hinreichend gesichert sind und die sich z.B. nicht im geschützten Netz der Bibliothek befinden, sondern in einem separaten Netzwerksegment, in dem sich z.B. auch die Nutzer-PCs befinden. Dies trifft i.d.R. aber nicht auf die in Auskunftssituationen genutzten Mitarbeiter-PCs zu.

Die FAG TI empfiehlt, die Mitarbeiter*innen zu informieren, dass USB-Medien von Nutzer*innen nicht an Auskunfts-PCs angeschlossen werden dürfen. Ggf. ist dies durch technische Maßnahmen (Unzugänglichmachung der USB-Ports) zu unterstützen, wenn zum Beispiel auch studentische Hilfskräfte und andere häufig wechselnde Personalgruppen in der Auskunft eingesetzt werden. Diese Maßnahme verhindert übrigens auch technische Schäden an den PCs, die durch defekte USB-Geräte auftreten können. Weiterhin ist es empfehlenswert, Maßnahmen zu überlegen, anhand derer der Bedarf des Zugriffs auf Nutzer-USB-Medien reduziert werden kann. So können zum Beispiel im Auskunftsgespräch recherchierte E-Medien den Nutzenden je nach Rechtssituation per Cloudlaufwerk oder Mail zur Verfügung gestellt werden, statt sie auf einem mitgebrachten USB-Stick zu speichern.

Kommunikationsfähigkeit im Notfall sicherstellen

Um Basis-Dienste auch bei einem Angriff aufrechtzuerhalten, sind präventive Maßnahmen und Notfallpläne entscheidend. Dazu gehört die regelmäßige Sicherung von Daten sowie der Aufbau redundanter Systeme, die im Ernstfall einspringen können.

- Im Falle eines schwerwiegenden IT-Sicherheitsvorfalls kann die eigene Kommunikationsinfrastruktur in der Form betroffen sein, dass die gewohnten Kommunikationswege wie Telefon, E-Mail und Website nicht mehr zur Verfügung stehen.
- Für die interne Kommunikation kann ein externes Chat- und Videokonferenzsystem genutzt werden. Die Zugangsdaten sollten auch dann zur Verfügung stehen, wenn die normalen Arbeitsplatz-PCs nicht mehr verfügbar sind.
- Die Website ist für die externe Kommunikation sehr wichtig. Wird diese in der eigenen Umgebung betrieben wird, ist eine extern betriebene Notfall-Webseite eine gute Möglichkeit, kommunikationsfähig zu bleiben. Für die Krisenkommunikation empfiehlt sich die Nutzung eines FAQ.
- Die telefonische Erreichbarkeit kann unabhängig von der eigenen Infrastruktur über Mobiltelefone realisiert werden. Weitere Mobiltelefone können für den zusätzlichen Bedarf im Notfall vorgehalten werden. Das Telefonverzeichnis sollte am besten auch ausgedruckt vorliegen.

Backup-Systeme und Systeme zur Servervirtualisierung nicht in die Windows-Domäne integrieren

Durch die Trennung dieser Systeme von der Domäne wird das Risiko minimiert, dass ein kompromittiertes Benutzerkonto oder ein Angriff auf die Domäne direkten Zugriff auf kritische Systeme erhält. Zudem bleibt die Verfügbarkeit der Backup- und Virtualisierungslösungen bei Domänenproblemen gewährleistet, was den Schutz vor Datenverlust und Ausfallzeiten verbessert.

Zwei Faktor Authentifizierung

Für wichtige und zentrale Dienste sollte neben dem Passwort ein zweiter, davon unabhängiger Faktor für die Anmeldung verlangt werden. Das kann z.B. ein mobiles Endgerät, ein biometrischer Faktor (Fingerabdruck), eine TAN-Liste oder ein spezieller USB-Stick sein. Mit diesem Vorgehen wird es Angreifenden, die z.B. über Phishing versuchen Windows-Kennungen zu erbeuten, schwer gemacht.

Sicherheitsmaßnahmen in Rechenzentren und großen Rechnernetzen

Für den Betrieb von Rechenzentren (und dazugehören auch Serverräume in Bibliotheken) existierten zahlreiche Maßnahmen, die die IT-Sicherheit stark erhöhen. Eine umfassende Liste anzugeben würde den Rahmen dieses Dokumentes sprengen, zumal viele Bibliotheken kein eigenes Rechenzentrum betreiben, sondern die Netzwerkumgebung von übergeordneten Organisationen mitnutzen. Trotzdem möchten wir hier auf einige etablierte Methoden hinweisen, die die Sicherheit insbesondere gegenüber Ransomware-Angriffen erhöhen können:

- Virenscanner: Mit Virenscannern, die auf spezifischen Systemen installiert werden (z.B. Upload-Server) können bekannte Schadsoftwares erkannt und isoliert werden.
- Schwachstellenscanner: Bestimmte Software-Tools wie z.B. Greenbone erlauben regelmäßige Scans nach bekannten Schwachstellen im eigenen Netzwerk. Angreifbare Systeme können gesichert oder vom Netz genommen werden.
- SIEM: Security Information and Event Management-Systeme (SIEM) erlauben die Überwachung von Rechnernetzen in Hinblick auf mögliche Angriffe wie die Verbreitung von Schadsoftware.
- Audits: Sicherheitsexperten können gebeten werden, Angriffe auf das Netzwerk / Rechenzentrum zu simulieren und auf diese Weise Sicherheitsprobleme zu erkennen.
- Honeypots: Dies sind scheinbar verwundbare Systeme, die im Netzwerk betrieben werden. Wenn Angreifer, die das Netzwerk bereits kompromittiert haben auf der Suche nach Sicherheitslücken auf die Honeypots zugreifen, werden die Systemadministrator*innen automatisch über diese Aktivität informiert und können Gegenmaßnahmen einleiten.

Zero Trust

Ein Zero Trust-Konzept, siehe dazu u. a. BSI – Zero Trust, setzt eine Software-Landschaft voraus, die nach Vorgaben für den generellen und minimal gehaltenen Zugriff auf Systeme und Daten („Least Privileges“) und unter Einbezug unterschiedlicher Kriterien, z. B. aktuelle Bewertung der Sicherheit eines Systems, überhaupt nur den Zugriff darauf erlaubt und somit jedes System zu einer verwalteten und kontrollierbaren Umgebung macht. Damit ist die Idee

einer Demilitarisierte Zone (DMZ, zentrale Firewall), also eines Perimeters, der Extern (nicht vertrauensvoll) von Intern (vertrauensvoll) trennt, hinfällig, da jedes System selbst zum Sicherheitsperimeter wird. Und zunehmend genutzte externe Dienste können unter dem gleichen Paradigma (einfacher) als „vertrauensvoll“ in die eigene Infrastruktur eingebunden werden.
Bis zu einer realistischen wie flächendeckenden Umsetzung einer solchen Software-Landschaft (die auch weiterhin zentrale Komponenten wie ein Identity und Access Management (IAM) beinhaltet) sollten folgende Maßnahmen, i. d. R. durch das Rechenzentrum, ergriffen werden:

- Zentrale Registrierung von Diensten und ihre Freigabe nur nach Sicherheitsüberprüfung
- Regelmäßige Sicherheitsüberprüfung registrierter Dienste / von Systemen (Schwachstellenscanner) und Benachrichtigung Verantwortlicher über gefundene und zu schließende Sicherheitslücken
- Zentrale Isolierung oder Abschaltung risikobehafteter Systemen, u. a. dann, wenn Sicherheitsprobleme nicht (in einem gegebenen Zeitrahmen) gelöst werden (können)
- Einsatz einer Lösung für Endpunktsicherheit (Endpoint Protection), um möglichst alle IT-Systeme auf Sicherheitsvorfälle zentral überwachen und ggf. isolieren und abschalten zu können (Virenscanner sind dabei nur ein Teilaspekt!)
- Ausbau / Umbau des Identity Managements (IDM) zu einem IAM, das möglichst feingranular den Zugriff auf Dienste und ihre Komponenten für berechtigte Personen, und diese Personen auch selbst, verwaltet
- Segmentierung des Netzwerks, um bei Sicherheitsvorfällen „Flächenbrände“ zu vermeiden

- BSI – Zero Trust
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Zero-Trust/zero-trust_node.html
  & Management-Blitzlicht Zero Trust
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Management_Blitzlicht/Management_Blitzlicht_Zero_Trust.pdf?__blob=publicationFile&v=6
  & Positionspapier Zero Trust 2023
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/Zero-Trust/Zero-Trust_04072023.pdf?__blob=publicationFile&v=4
- Begriffsentwicklung: No More Chewy Centers: Introducing The Zero Trust Model Of Information Security, Forrester Analyst John Kindervag, 2010
  https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf