Il ruolo della cybersecurity per le biblioteche digitali: sfide attuali e strategie di protezione

«Dig*Italia*» 2-2024
DOI: 10.36181/digitalia-00104

Anna Maria Tammaro – *Università di Parma*
Emanuele Bellini – *Università Roma Tre*

Comprendere la cybersecurity nel dominio del patrimonio culturale e affrontare le minacce in continua evoluzione alle biblioteche digitali è diventato imperativo per garantire la loro sostenibilità e affidabilità. Questo articolo esplora il complesso panorama della cybersecurity nelle biblioteche digitali, identificando le principali sfide e vulnerabilità, e presentando strategie per proteggere i depositi digitali e salvaguardare la privacy degli utenti. Particolare attenzione è dedicata al ruolo fondamentale dei bibliotecari consapevoli delle problematiche legate alla sicurezza informatica, i quali non solo implementano misure protettive, ma educano gli utenti e responsabilizzano le comunità, consentendo loro di interagire con fiducia con le risorse delle biblioteche digitali in un ambiente sempre più interconnesso e vulnerabile.

1. Background e introduzione

Nella società dell'informazione, le biblioteche digitali sono diventate piattaforme fondamentali per la creazione, la conservazione, l'accesso e la diffusione della conoscenza. Queste gestiscono una vasta gamma di risorse e dati – libri, articoli, manoscritti, immagini e materiali multimediali – che devono essere resi accessibili a un pubblico globale. Tuttavia, la crescente dipendenza dalle tecnologie digitali le espone inevitabilmente a una varietà di minacce informatiche in continua evoluzione.

Tradizionalmente, si è ritenuto che le biblioteche digitali non rappresentassero un obiettivo appetibile per il cybercrime. Questa percezione largamente diffusa ha portato il dibattito, specialmente nel contesto umanistico, a concentrarsi su problematiche più "tradizionali", come la conservazione digitale a lungo termine e l'autenticità dei documenti. Tuttavia, questa sensazione di sicurezza è sempre più messa in discussione dai fatti.

Episodi recenti, come gli attacchi informatici a importanti biblioteche negli Stati Uniti, l'incidente clamoroso alla British Library e i cyber attacchi al Louvre e ad altri musei francesi durante le Olimpiadi del 2024, hanno dimostrato quanto vulnerabili possano essere queste istituzioni. Questi eventi, richiamano con urgenza l'attenzione sull'impatto potenzialmente devastante di tali attacchi, non solo in termini di perdita di dati, ma anche di interruzione dei servizi essenziali.

È quindi necessario che la cybersecurity diventi una componente fondamentale della gestione delle biblioteche digitali. Occorre sviluppare una consapevolezza diffusa delle principali sfide in questo ambito e adottare strategie proattive per mitigare i rischi, proteggendo così non solo i contenuti, ma anche il ruolo centrale di queste istituzioni nella società digitale.

La cybersecurity, o sicurezza informatica, è definita come il processo di protezione delle informazioni e dei dati per garantire riservatezza, integrità e disponibilità (ISO 27000:2018). Oltre ai principi fondamentali della cybersecurity – riservatezza, integrità e disponibilità – esistono altre dimensioni che ampliano e rafforzano la capacità di un sistema di sicurezza informatica di proteggere non solo i dati, ma anche la reputazione e la fiducia che gli utenti ripongono nell'istituzione.
Questi aspetti includono:
Autenticità: garantire che i dati, i sistemi e le comunicazioni siano genuini e provenienti da fonti affidabili. Per una biblioteca digitale, questo significa assicurarsi che i contenuti siano autentici e non alterati, salvaguardando così la credibilità dell'istituzione.
Responsabilità (Accountability): assicurare che ogni azione o decisione relativa alla gestione dei dati sia attribuibile a un soggetto specifico. Questo principio promuove la trasparenza e offre un elemento di fiducia per gli utenti, che possono essere certi che i dati siano gestiti in modo corretto e tracciabile.
Non ripudio: Garantire che nessuna delle parti coinvolte in una comunicazione o transazione digitale possa negare la propria partecipazione. Ad esempio, un amministratore non può negare di aver modificato un certo dato, proteggendo così l'integrità delle operazioni e la fiducia nel sistema.
Affidabilità (Reliability): Assicurare che i sistemi e i servizi funzionino in modo coerente e prevedibile, offrendo un accesso stabile e continuo. Questo è cruciale per mantenere la reputazione di una biblioteca digitale come fonte affidabile e sempre disponibile.

Queste dimensioni non riguardano solo la sicurezza tecnica, ma incidono profondamente sulla percezione pubblica e sulla reputazione della biblioteca digitale. La perdita di dati o l'alterazione di contenuti non autentici possono compromettere non solo la funzionalità del sistema, ma anche la fiducia degli utenti e il ruolo della biblioteca digitale come custode di conoscenza e cultura.
L'integrazione di queste dimensioni nel sistema di sicurezza di una biblioteca digitale consente di affrontare non solo le minacce tecniche, ma anche le esigenze di fiducia e trasparenza, creando così un sistema robusto e resiliente capace di resistere agli attacchi e mantenere l'integrità delle informazioni.
Nelle biblioteche digitali, tali principi non solo sono cruciali, ma diventano determinanti per affrontare le sfide specifiche legate alla conservazione digitale e alla tutela della privacy degli utenti. Minacce come violazioni o alterazioni dei dati, accessi non autorizzati e perdite di informazioni rappresentano rischi concreti che possono compromettere la fiducia degli utenti nell'istituzione e nella conoscenza che essa custodisce.
Tra questi aspetti, l'integrità dei dati assume un'importanza particolare nell'era della post-verità, in cui la manipolazione delle informazioni può avere conseguenze imprevedibili e di vasta portata. Garantire che i contenuti digitali siano autentici e non alterati è essenziale per preservare il ruolo delle biblioteche come custodi della conoscenza e come fonti affidabili in una società sempre più interconnessa.

1.1. Attacco informatico alla British Library, al Louvre e al Gran Palace
Il recente attacco alla British Library ha evidenziato la necessità di dare priorità alla sicurezza informatica dei beni culturali in generale e delle biblioteche digitali in particolare. La British Library ha subito uno degli attacchi più gravi a un'istituzione del patrimonio culturale. Il famigerato gruppo Ransomware Rhysida, responsabile dell'attacco, ha copiato ed esfiltrato (cioè rimosso illegalmente) circa 600 GB di file, inclusi dati personali di utenti e personale della biblioteca. Sebbene la biblioteca si stia lentamente riprendendo e abbia ammirevolmente pubblicato

apertamente un suo documento di riflessione sulle lezioni apprese dall'evento informatico[1], l'incidente ha evidenziato la drammatica necessità di avere nuove competenze tecniche per la sicurezza informatica della biblioteca digitale. Oltre all'esfiltrazione dei dati a scopo di riscatto, i metodi degli aggressori hanno incluso la crittografia di dati e dei sistemi e la distruzione di alcuni server per impedire il ripristino del sistema e coprire le proprie tracce. Quest'ultima azione ha avuto l'impatto più dannoso sulla biblioteca: sebbene la British Library disponesse di copie sicure di tutte le collezioni digitali, inclusi i contenuti digitali e quelli digitalizzati coi metadati che li descrivono, il ripristino è stato ostacolato dalla mancanza di infrastrutture valide a causa della loro dipendenza da un numero significativo di applicazioni "legacy" obsolete[2].

Nonostante l'incidente alla British Library, l'approccio delle biblioteche digitali e delle istituzioni culturali in generale non è cambiato in modo significativo. Questa mancanza di attenzione è stata ulteriormente evidenziata durante le Olimpiadi di Parigi del 2024, quando un attacco ransomware ha colpito il Museo del Louvre, il Grand Palais e altre importanti istituzioni culturali francesi. L'obiettivo degli attaccanti era estorcere un riscatto e, potenzialmente, vendere dati sensibili, compromettendo così la privacy degli utenti.

Tuttavia, l'attenzione pubblica e istituzionale si è concentrata prevalentemente sui rischi per i sistemi che gestivano i Giochi olimpici, trascurando la gravità di un attacco informatico contro le istituzioni culturali più prestigiose del Paese. Questo episodio mette in luce una sottovalutazione diffusa dell'impatto che i cyber attacchi possono avere su biblioteche e musei digitali, non solo in termini di perdita di dati o funzionalità, ma anche rispetto alla fiducia degli utenti e alla reputazione delle istituzioni stesse.

Lo studio si pone l'obiettivo di sensibilizzare su queste sfide critiche, promuovendo una maggiore consapevolezza della necessità di implementare strategie e buone pratiche di cybersecurity nelle istituzioni culturali per mitigare i rischi e prevenire danni futuri.

2. Metodologia: rassegna della letteratura

Per raggiungere gli obiettivi dello studio, la metodologia adottata si è basata sulla rassegna della letteratura. È stata condotta una revisione sistematica della letteratura usando le banche dati di IEEE Xplore Digital Library, Taylor & Francis, Emerald Insight, Scopus, Wiley Online Library, ACM Digital Library, Google Scholar. La letteratura sulla cybersecurity nelle biblioteche digitali è appena agli inizi, con ricerche che coprono vari aspetti della protezione dei dati e delle infrastrutture digitali (Anday et al. 2012; Huang et al. 2019; Han et al. 2016). La maggioranza degli studi hanno evidenziato un approccio reattivo con la consapevolezza dell'importanza di proteggere i dati sensibili degli utenti e di garantire la continuità dei servizi in caso di attacchi informatici (Kim 2016). Tuttavia, c'è un crescente riconoscimento della necessità di sviluppare approcci più sofisticati e proattivi per affrontare le minacce emergenti, come il Ransomware e le violazioni della privacy.

I risultati della rassegna della letteratura sono descritti in due paragrafi: le sfide con le vulnerabilità da affrontare e le strategie con le buone pratiche messe in atto dalle biblioteche digitali.

[1] Si veda: British Library, *Learning lessons from the cyber-attack*, 2024, <https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf>.

[2] «Un sistema legacy, in informatica, è un sistema informatico, un'applicazione o un componente obsoleto, che continua ad essere usato poiché l'utente non intende o non può rimpiazzarlo. Legacy equivale a versione "retrodatata". In italiano può essere tradotto con "obsoleto", "vecchio" o "fuori commercio», in: Wikipedia, <https://it.wikipedia.org/wiki/Sistema_legacy>.

3. Sfide per la sicurezza informatica delle biblioteche digitali

La biblioteca digitale non è semplicemente un deposito digitale per l'archiviazione e la catalogazione di contenuti digitali. Nel nostro mondo sempre più interconnesso, in cui i confini tra fisico e digitale sono sfumati, le biblioteche digitali svolgono un ruolo cruciale nella creazione, conservazione e condivisione della conoscenza. Sono parti integranti di un complesso sistema di infrastruttura socio tecnologica (umano-cyber-fisico), incaricato di salvaguardare le informazioni e garantire l'affidabilità e l'accessibilità. In quanto tali, le biblioteche digitali dovrebbero essere riconosciute come infrastrutture critiche per la conoscenza, simili per importanza strategica ai sistemi di trasporto e ai sistemi energetici.
Tuttavia, come qualsiasi infrastruttura, questa centralità le rende anche particolarmente vulnerabili a una serie di minacce e sfide specifiche che includono: accesso e autenticazione, protezione dei dati, minacce interne ed esterne, Ransomware, attacchi DDoS (Distributed Denial-of-Service), alterazione degli oggetti digitali:

Accesso e autenticazione: garantire che solo utenti autorizzati possano accedere alle risorse, mantenendo al contempo un equilibrio tra sicurezza e usabilità.

Protezione dei dati: salvaguardare i dati archiviati e condivisi da perdite, corruzioni o accessi non autorizzati, proteggendo al contempo la privacy degli utenti.

Minacce interne ed esterne: affrontare i rischi provenienti da attori interni (ad esempio, errori o azioni dolose di dipendenti) e da attacchi esterni (hacker, malware[3]).

Attacchi Ransomware[4]: contrastare il rischio che dati essenziali vengano criptati e resi inaccessibili fino al pagamento di un riscatto.

Attacchi DDoS (Distributed Denial-of-Service): Prevenire azioni volte a sovraccaricare i server, rendendo i servizi inaccessibili agli utenti.

Alterazione degli oggetti digitali: impedire la manipolazione dei contenuti digitali, che potrebbe compromettere la fiducia degli utenti nella validità delle risorse fornite.

3.1 Le vulnerabilità delle biblioteche digitali

La vulnerabilità primaria delle biblioteche digitali risiede nella loro intricata rete di interdipendenze, strettamente intrecciate nel tessuto dell'infrastruttura critica per la conoscenza. Le biblioteche digitali spesso condividono risorse, metadati e sistemi di autenticazione con istituti accademici e di ricerca, creando opportunità per gli aggressori di sfruttare queste connessioni e infiltrarsi simultaneamente in più reti o repository di dati. I Linked Open Data, una caratteristica del successo delle biblioteche digitali, si basano sulla presunzione di accessibilità e affidabilità continue. Tuttavia, un attacco a un nodo all'interno di questo sistema può innescare effetti a ca-

[3] Malware indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer. Termine coniato nel 1990 da Yisrael Radai, precedentemente veniva chiamato virus per computer.

[4] Il ransomware è un programma informatico dannoso ("malevolo") che può "infettare" un dispositivo digitale (PC, tablet, smartphone), bloccando l'accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file ecc.) per poi chiedere un riscatto (in inglese, "ransom") da pagare per "liberarli".

scata, sia fisici (ad esempio, guasti del server, corruzione dei dati) che sociali (ad esempio, perdita di fiducia nelle informazioni, suscettibilità ai dati manipolati), con profonde implicazioni per la ricerca e la società.

Inoltre, le biblioteche digitali rappresentano obiettivi allettanti per gli attacchi informatici a causa della ricchezza di dati che custodiscono, tra cui documenti di ricerca, documenti storici unici, informazioni personali e documenti protetti dalla proprietà intellettuale. Gli aggressori possono agire per fini economici oppure avere obiettivi ideologici, fare spionaggio o semplicemente mirare a interrompere le operazioni. Software dannosi, come Malware e Ransomware, possono compromettere l'integrità dei dati e limitare l'accesso alle risorse. Gli attacchi Denial-of-Service (DoS) possono interrompere i servizi sovraccaricando i server con il traffico.

Il Regolamento generale sulla protezione dei dati (GDPR), che si applica in tutta l'Unione Europea (UE), regola il trattamento dei dati personali e ha un impatto sul modo in cui le biblioteche digitali gestiscono e proteggono i dati degli utenti. Le biblioteche digitali devono rispettare i requisiti del GDPR in merito alla raccolta, all'archiviazione, al trattamento e al consenso dei dati. Le violazioni sulla protezione dei dati protetti comportano rischi di esposizione di informazioni sensibili, mentre gli schemi di phishing prendono di mira gli operatori per ottenere un accesso non autorizzato. Inoltre, le minacce interne, in cui alcuni individui abusano dei propri privilegi di accesso, sono una preoccupazione ulteriore. Il mancato aggiornamento tempestivo dei sistemi può lasciare le biblioteche vulnerabili, come si è visto nell'evento di violazione informatica del 2023 presso la British Library.

Aggravato dall'uso di software obsoleti e sistemi legacy con vulnerabilità note, le biblioteche digitali sono esposte a rischi elevati di accesso non autorizzato, manipolazione dei dati e altre attività dannose di cybersecurity. Le conseguenze di tali attacchi possono essere finanziariamente gravose e impedire il ritorno alle normali operazioni in tempi ragionevoli.

Inoltre, un falso senso di sicurezza circonda le risorse ad accesso aperto, poiché la loro apertura non le rende immuni da manomissioni. Infatti, i contenuti ad accesso aperto alterati possono diffondersi rapidamente nel panorama digitale globale, ponendo sfide per la loro individuazione e le relative azioni di difesa. Gestire la sicurezza di diversi formati di contenuto, tra cui testo, immagini, audio e video, mette ulteriormente a dura prova le risorse e le competenze di sicurezza informatica all'interno delle biblioteche digitali.

Le potenziali conseguenze di un attacco informatico riuscito a una biblioteca digitale abbracciano diversi domini critici. Una delle preoccupazioni principali è la potenziale perdita o il furto di preziose collezioni/dati del patrimonio, che comprendono documenti di ricerca, documenti storici unici, informazioni personali degli utenti, proprietà intellettuale e altri contenuti sensibili. Nei casi in cui la copia digitale funge da unica versione rimanente di un oggetto fisico non più disponibile, qualsiasi perdita o alterazione di questa copia comporta la sua irreversibile distruzione o alterazione del patrimonio - e quindi della memoria - le cui implicazioni di medio e lungo periodo possono essere immaginabili.

Un altro impatto significativo è la corruzione, che porta a inesattezze, compromissione dell'integrità o inutilizzabilità dei dati, ma uno dei rischi emergenti critici è correlato alla manipolazione del patrimonio culturale (in pratica tramite l'intelligenza artificiale). Inoltre, un attacco informatico può interrompere i servizi digitali, rendendo le collezioni inaccessibili agli utenti e influenzando la ricerca, l'istruzione e altre attività che dipendono dalla disponibilità delle risorse digitali. Possono sorgere implicazioni finanziarie dovute alle spese associate alla risposta agli incidenti, al recupero dei dati, alle spese legali, alle sanzioni normative e alla potenziale perdita di entrate o finanziamenti.

Inoltre, un attacco informatico può rovinare la reputazione della biblioteca digitale, diminuendone la credibilità e l'affidabilità tra utenti, ricercatori, istituzioni accademiche, agenzie di finanziamento e il pubblico in generale. A seconda della natura della violazione e delle normative pertinenti, come il GDPR, la biblioteca digitale potrebbe dover affrontare conseguenze legali, tra cui multe, azioni legali e sanzioni normative per non aver salvaguardato adeguatamente le informazioni sensibili.
Infine, le biblioteche digitali spesso ospitano risorse con proprietà intellettuali di valore, tra cui materiali protetti da copyright, risorse proprietarie e opere inedite, che potrebbero essere oggetto di furto o distribuzione non autorizzata, con conseguenti perdite finanziarie e danni alla reputazione dei creatori di contenuti e dei titolari dei diritti.

4. Strategie per la sicurezza informatica delle biblioteche digitali

Per proteggere efficacemente le biblioteche digitali, è essenziale implementare una serie di strategie di cybersecurity, declinate sulle caratteristiche dell'organizzazione che deve essere aperta per natura. L'implementazione di protocolli di autenticazione robusti, crittografia, formazione e sensibilità di staff e utenti, sistemi di monitoraggio e risposta agli eventi sono solo alcuni aspetti che la ricerca sulla sicurezza informatica delle biblioteche digitali dovrebbe esplorare.
L'attacco alla British Library dimostra che molte biblioteche digitali, anche quelle prestigiose, non sono attrezzate per affrontare le crescenti minacce provenienti dal dominio informatico. Spesso non vengono utilizzate tecnologie già in uso in altre infrastrutture critiche, come i sistemi di Security Information and Event Management (SIEM) o sistemi avanzati di rilevamento delle anomalie o strumenti di scansione delle vulnerabilità. In genere, le istituzioni culturali si concentrano principalmente sulla *business continuity* per mitigare gli effetti di guasti accidentali del sistema. È evidente che solo questo approccio reattivo non è più valido per affrontare le minacce alla sicurezza emergenti.
Il cambio di paradigma richiesto dagli ultimi incidenti informatici dovrà consentire di migliorare non solo la dotazione tecnologica di una biblioteca digitale, ma anche l'organizzazione istituzionale e le competenze dello staff per la sicurezza e la difesa informatica.

4.1 Accesso e autenticazione

Prima di tutto, le biblioteche digitali dovrebbero stabilire policy di controllo degli accessi che delineino ruoli, permessi e privilegi per personale, appaltatori e utenti, rispettando il principio del privilegio minimo. L'accesso dovrebbe essere concesso esclusivamente in base alla necessità, limitando l'accesso ai dati sensibili all'essenziale.
L'implementazione di meccanismi di autenticazione robusti, come l'autenticazione multifattoriale (MFA) o l'autenticazione biometrica, può verificare l'identità degli utenti quando accedono a informazioni, migliorando la tracciabilità e prevenendo accessi illeciti.
Per monitorare e verificare in modo efficace le attività degli utenti, comprese quelle dei fornitori e dei collaboratori terzi, nonché i modelli di accesso e le modifiche ai dati sensibili, è essenziale implementare meccanismi di monitoraggio e verifica completi. Ciò comporta la registrazione delle azioni degli utenti, il monitoraggio del traffico di rete e l'esecuzione di verifiche di routine delle autorizzazioni di accesso e dell'utilizzo.
Inoltre, è fondamentale implementare soluzioni di Data Loss Prevention (DLP) per supervisionare e regolare lo spostamento di dati sensibili all'interno dell'ambiente della biblioteca digitale.
L'applicazione di meccanismi di controllo degli accessi basati sui ruoli è un altro aspetto fondamentale, che garantisce controlli degli accessi granulari basati sui ruoli, sulle responsabilità e

sulla gerarchia organizzativa degli utenti. Il controllo degli accessi basato sui ruoli (RBAC) garantisce che gli individui accedano solo alle informazioni pertinenti alle loro funzioni lavorative. Per soluzioni più avanzate come Behavioral Analytics, la loro implementazione dovrebbe essere valutata solo se l'analisi dei rischi la giustifica.

4.2 Formazione e consapevolezza del personale e degli utenti

L'elemento umano all'interno di un sistema umano-cyber-fisico ha un'importanza fondamentale (Fox – El Sherbiny 2011; Kont 2024). Infatti, come indicato da un rapporto IBM[5], quasi tutti gli attacchi informatici derivano da azioni intenzionali o non intenzionali di individui che operano all'interno del sistema.

La formazione in cybersecurity deve essere considerata una priorità strategica per le biblioteche digitali. Le competenze di base in questo ambito dovrebbero diventare un elemento essenziale nella preparazione dei bibliotecari, mentre conoscenze più avanzate potrebbero arricchire l'offerta formativa di percorsi accademici orientati alla transdisciplinarità, come i corsi per bibliotecari digitali o quelli di informatica umanistica. Parallelamente, è indispensabile che il personale delle biblioteche e gli utenti siano regolarmente formati e aggiornati per comprendere e applicare le best practice di sicurezza, che evolvono costantemente per rispondere alle nuove minacce.

Gli utenti stessi, tra cui ricercatori, studenti e altri stakeholder, possono rappresentare un rischio per la sicurezza informatica, spesso senza esserne consapevoli. Azioni come cliccare su link malevoli, cadere vittime di phishing o utilizzare password deboli sono esempi comuni di vulnerabilità introdotte inconsapevolmente. Sebbene sia fondamentale che i sistemi impongano misure di sicurezza per mitigare tali rischi, è altrettanto importante evitare restrizioni che possano ostacolare le normali attività operative. Di conseguenza, le biblioteche digitali devono implementare soluzioni che non solo proteggano i dati e i sistemi, ma che guidino gli utenti verso comportamenti sicuri, come la scelta di password robuste e univoche o l'adozione dell'autenticazione a più fattori (MFA) quando disponibile.

Questi sforzi devono essere integrati in una cultura organizzativa improntata alla consapevolezza e alla responsabilità in materia di sicurezza informatica. Tale cultura dovrebbe promuovere una gestione proattiva del rischio, l'apprendimento continuo e la partecipazione attiva di tutto il personale e degli utenti. Solo attraverso un impegno collettivo sarà possibile proteggere in modo efficace il patrimonio culturale digitale, garantendo al contempo un accesso sicuro e senza ostacoli alla conoscenza.

4.3 Crittografia dei dati

La crittografia rappresenta uno degli strumenti più efficaci per garantire la sicurezza dei dati, specialmente in un contesto come quello delle biblioteche digitali, dove grandi quantità di informazioni sensibili e risorse di valore intellettuale devono essere salvaguardate. Convertendo i dati in un formato illeggibile, decifrabile solo attraverso una chiave crittografica corretta, la crittografia non solo protegge la riservatezza delle informazioni, ma costituisce una difesa fondamentale contro accessi non autorizzati, anche in caso di violazione dei sistemi di archiviazione o trasmissione. Numerosi quadri normativi e standard di settore, come GDPR, HIPAA, FERPA e PCI DSS[6], impongono alle organizzazioni di incorporare la crittografia nelle loro strategie di protezione dei dati.

[5] https://www.ibm.com/downloads/cas/A27KQP8R.

[6] HIPAA (Health Insurance Portability and Accountability Act); FERPA (Family Educational Rights and Privacy Act); PCI DSS (Payment Card Industry Data Security Standard).

Ciò impedisce efficacemente l'accesso non autorizzato da parte di aggressori informatici o malintenzionati, anche se riescono a violare i canali di archiviazione o trasmissione. Tuttavia, l'implementazione della crittografia richiede una valutazione approfondita della sua convenienza.
Quando si parla di sicurezza informatica, la crittografia può essere applicata in due momenti principali. Da un lato, protegge i dati a riposo, ovvero quelli archiviati su server, database o dispositivi di archiviazione fisici. Questo è cruciale per le biblioteche digitali, perché garantisce che i dati rimangano inutilizzabili anche se sistemi o dispositivi vengono compromessi.
Ad esempio, le biblioteche digitali solitamente ospitano grandi quantità di dati sensibili, tra cui documenti di ricerca, manoscritti, informazioni personali e risorse con proprietà intellettuale. La crittografia dei dati a riposo salvaguarda questi dati mentre risiedono su server, database o dispositivi di archiviazione, proteggendoli da accessi non autorizzati in caso di violazione della sicurezza o furto fisico.
Al contrario, la crittografia è essenziale durante la trasmissione dei dati attraverso reti come Internet o infrastrutture interne, dove i dati sono suscettibili di intercettazione.
La crittografia dei dati in transito, spesso ottenuta tramite protocolli come Transport Layer Security (TLS) o Secure Sockets Layer (SSL), crittografa i dati durante il loro percorso, garantendo sia riservatezza che integrità.
Nelle biblioteche digitali chiuse, come quelle che offrono accesso su abbonamento (ad esempio, IEEE Xplore), la crittografia non solo protegge i dati sensibili, ma contribuisce anche a salvaguardare il valore commerciale delle risorse. Tuttavia, nelle biblioteche digitali che offrono contenuti open access, la crittografia potrebbe essere percepita come un ostacolo al libero flusso di conoscenza. Per questo motivo, è essenziale considerare il contesto specifico e bilanciare la necessità di protezione dei dati con la missione di accessibilità e condivisione del sapere. In sintesi, la crittografia non è solo un'opzione, ma una componente essenziale della sicurezza informatica per le biblioteche digitali. Tuttavia, la sua applicazione deve essere attentamente bilanciata con la missione delle biblioteche digitali di promuovere l'accesso e la diffusione della conoscenza.
L'efficacia della crittografia dipende anche dalla sensibilizzazione degli utenti e del personale. Strumenti sofisticati possono risultare inefficaci se accompagnati da comportamenti che mettono a rischio la sicurezza, come la condivisione non autorizzata delle chiavi crittografiche o la mancata adozione di protocolli sicuri. Inoltre, l'implementazione di sistemi crittografici può comportare costi significativi e introdurre complessità operative che vanno attentamente bilanciate rispetto al valore delle risorse protette. In definitiva, la crittografia non rappresenta solo una soluzione tecnica, ma una strategia chiave per garantire la sicurezza delle biblioteche digitali. Tuttavia, la sua applicazione deve essere ponderata per rispettare l'equilibrio tra protezione dei dati e libero accesso alla conoscenza, mantenendo sempre al centro l'obiettivo di preservare la fiducia degli utenti.

4.4 Privacy

L'aderenza alle normative sulla protezione dei dati, come il Regolamento generale sulla protezione dei dati (GDPR), rappresenta una responsabilità cruciale per le biblioteche digitali. Queste istituzioni devono considerare attentamente l'impatto delle normative sulla gestione delle loro operazioni, adottando misure concrete per garantirne la conformità. Un primo passo essenziale consiste nell'effettuare un inventario approfondito e una valutazione dei dati personali trattati dalla biblioteca digitale, identificando e categorizzando le informazioni raccolte, archiviate, elaborate e trasmesse. Questo processo è indispensabile per definire con precisione le responsabilità e le azioni necessarie per la protezione dei dati.

In parallelo, le biblioteche digitali devono sviluppare politiche e avvisi sulla privacy chiari e trasparenti, articolando le finalità del trattamento dei dati e offrendo agli utenti opzioni di consenso esplicito, come l'opt-in o l'opt-out. Tali misure non solo rafforzano la conformità normativa, ma migliorano anche la fiducia degli utenti nei confronti dell'istituzione. La trasparenza e il rispetto per le scelte individuali degli utenti diventano così elementi integranti della strategia di gestione dei dati.
Per garantire la conformità nel tempo, è essenziale implementare un monitoraggio regolare tramite audit, valutazioni e revisioni delle policy, delle procedure operative e delle attività di trattamento dei dati. Questi controlli sistematici permettono di identificare eventuali lacune e di adottare le misure correttive necessarie. In caso di violazioni dei dati o di incidenti di non conformità, è indispensabile che siano predisposti meccanismi tempestivi e trasparenti per la segnalazione e la risoluzione, con l'obiettivo di minimizzare i danni e prevenire futuri problemi.
Infine, l'impatto della normativa per la privacy non si limita all'aspetto tecnico, ma influenza profondamente l'approccio complessivo delle biblioteche digitali alla sicurezza informatica. Integrare principi di privacy e protezione dei dati in ogni livello dell'organizzazione non solo garantisce il rispetto delle normative, ma contribuisce a costruire un ecosistema digitale più sicuro e orientato alla tutela degli utenti.

5. Verso una biblioteca digitale resiliente

Stabilire in modo efficace le priorità per gli investimenti e le risorse in materia di sicurezza informatica è un processo decisionale multicriterio che richiede alle biblioteche di valutare i propri rischi, vulnerabilità ed esigenze operative (Ngwum et al. 2020; Yin 2024). Fino ad oggi, le risorse sono state principalmente concentrate sull'archiviazione, conservazione (storage) e accessibilità, considerando nel migliore dei casi la sicurezza una commodity fornita dai servizi esterni su cui la biblioteca digitale si appoggia, oppure, nel peggiore dei casi, non considerandola affatto. Considerando la condizione costante di limitazione delle risorse in cui gli istituti culturali generalmente operano, spesso mancano investimenti.
L'obiettivo è trovare un equilibrio tra gli investimenti per l'operatività e le misure di sicurezza. L'allocazione delle risorse dovrebbe derivare da una valutazione del rischio integrata e dinamica, volta a identificare e classificare i rischi. Ciò comporta la valutazione delle vulnerabilità e del potenziale impatto di varie minacce note, ibride ed emergenti adottando però una visione socio-tecnologica della biblioteca digitale. In altri termini, l'impatto non deve essere solo valutato sull'operatività del servizio ma anche a livello sociale, vista la natura degli oggetti trattati. Per raggiungere questo obiettivo, è fondamentale adottare per le biblioteche digitali in particolare e per i beni culturali in generale, la prospettiva della biblioteconomia critica per le infrastrutture, intese come sistemi, reti e risorse fisiche o virtuali che sono essenziali per il funzionamento di una nazione. In questa ottica le biblioteche digitali rispondono ai tre criteri delle infrastrutture delle biblioteche per la biblioteconomia critica:

– Essenzialità: un paese o una società non potrebbero sopravvivere e progredire se perdessero la conoscenza su cui si basa il ruolo delle biblioteche digitali.
– Interdipendenza: le biblioteche digitali in quanto custodi della conoscenza di una società, sono intrinsecamente collegate a ogni aspetto del sapere e quindi della vita della società stessa.
– Impatto potenziale: la distruzione o l'alterazione del patrimonio culturale di un paese ha un impatto rilevantissimo sull'identità della comunità, sulla coesione e sulle attività.

In questa prospettiva, è cruciale passare da un approccio focalizzato esclusivamente sulla prevenzione degli incidenti (sicurezza) a un modello orientato alla mitigazione degli eventi avversi e al rapido recupero (resilienza). Questo cambio di paradigma non si limita a rafforzare le difese, ma introduce una visione più ampia e dinamica della gestione del rischio, che riconosce l'inevitabilità di alcuni attacchi e si concentra sulla capacità di rispondere e adattarsi efficacemente.
Framework consolidati, come quelli sviluppati dal NIST (National Institute of Standards and Technology) o dal NAS (National Academy of Sciences), forniscono linee guida essenziali per aiutare le organizzazioni a progettare una strategia resiliente e integrata. L'obiettivo principale è ridurre il divario tra il mantenimento delle operazioni della biblioteca digitale e il perseguimento della sua missione fondamentale di accesso alla conoscenza e salvaguardia del patrimonio culturale.
La resilienza informatica va oltre la semplice resistenza agli attacchi: richiede l'abilità di apprendere dagli incidenti, adattarsi al panorama delle minacce in continua evoluzione e migliorare continuamente le proprie capacità difensive. In questo contesto, spostare l'attenzione dalla pura conformità normativa a misure di sicurezza proattive e adattabili diventa una necessità strategica per garantire la sostenibilità e l'affidabilità delle biblioteche digitali nel lungo termine.
La resilienza informatica in genere comprende quattro fasi: preparazione, assorbimento, recupero e adattamento, ciascuna delle quali richiede azioni specifiche. Nella fase di preparazione, diventa essenziale condurre valutazioni del rischio e della capacità. Queste valutazioni prendono in esame vari fattori, tra cui i tipi di dati archiviati, i punti di accesso, l'infrastruttura di rete, le dipendenze di terze parti, gli obblighi normativi, la consapevolezza organizzativa, i livelli di competenza e i potenziali attori della minaccia.
Da questo framework emergono tre pilastri fondamentali per una strategia di cybersecurity efficace nelle biblioteche digitali: organizzazione, cultura della sicurezza e tecnologia.
Il primo pilastro, organizzazione, richiede la creazione di una solida struttura di governance per la sicurezza informatica. Ciò implica la definizione chiara di policy, ruoli e responsabilità, nonché la nomina di un Chief Information Security Officer (CISO) o di un responsabile della sicurezza informatica. Questo ruolo è essenziale per supervisionare le iniziative di sicurezza, coordinare gli sforzi tra i diversi dipartimenti, monitorare e aggiornare regolarmente le policy e garantire una comunicazione trasparente ed efficace con gli stakeholder interni ed esterni. Una governance ben strutturata crea le fondamenta per una gestione proattiva e resiliente della sicurezza informatica.
Il secondo pilastro si focalizza sulla consapevolezza e sulla cultura della sicurezza informatica, elementi essenziali per rafforzare la resilienza delle biblioteche digitali. Sessioni di formazione regolari rivolte al personale della biblioteca, a ricercatori, studenti e stakeholder sono indispensabili per sensibilizzare sui rischi informatici, promuovere le migliori pratiche e chiarire le responsabilità individuali nella protezione delle risorse e dei dati della biblioteca digitale.
Questo pilastro include anche un impegno attivo verso la collaborazione interistituzionale. Le biblioteche digitali, essendo parte di un complesso ecosistema umano-cyber-fisico con numerose interdipendenze, devono stabilire relazioni di fiducia ed efficaci con altri attori del sistema. Collaborazioni strutturate con università e istituti di ricerca possono offrire accesso a competenze, risorse e innovazioni nel campo della sicurezza informatica. Allo stesso modo, mantenere un contatto permanente con agenzie governative, forze dell'ordine, enti normativi e associazioni di settore consente di affrontare con maggiore efficacia le sfide della sicurezza informatica.
Al centro di queste collaborazioni deve esserci la condivisione di informazioni, che permette lo scambio di conoscenze su minacce emergenti, tendenze e strategie di mitigazione. Questa sinergia non solo rafforza la sicurezza delle singole biblioteche digitali, ma contribuisce a creare

un sistema resiliente e ben connesso, capace di rispondere proattivamente al panorama in continua evoluzione delle minacce informatiche.
Il terzo pilastro si concentra sull'implementazione di tecnologie appropriate, che costituiscono la base operativa della strategia di sicurezza delle biblioteche digitali. Tecnologie fondamentali come il controllo degli accessi e la gestione delle identità garantiscono che solo utenti autorizzati possano accedere alle risorse, mentre misure di sicurezza di rete, come firewall e sistemi di rilevamento e prevenzione delle intrusioni (IDPS), offrono protezione contro le minacce esterne. Tuttavia, è essenziale che queste tecnologie non si limitino alla prevenzione, ma includano strumenti capaci di attenuare l'impatto di eventuali attacchi e consentire un ripristino sicuro dei servizi.
Un esempio rilevante è rappresentato dall'architettura Zero Trust (Zero Trust Architecture, ZTA), un approccio che elimina il concetto di fiducia implicita, richiedendo una verifica rigorosa dell'identità e controlli di accesso per ogni utente, dispositivo o applicazione che tenta di accedere alle risorse. Adottando ZTA, le biblioteche digitali possono rafforzare la propria sicurezza mitigando i rischi legati ad accessi non autorizzati e proteggendo informazioni e risorse sensibili.
Un altro strumento indispensabile è rappresentato dalle soluzioni di Data Loss Prevention (DLP), progettate per prevenire la divulgazione o la fuga non autorizzata di dati sensibili. Questi sistemi monitorano, rilevano e applicano policy sull'uso, la condivisione e l'archiviazione dei dati, garantendo il rispetto delle normative sulla protezione dei dati, salvaguardando la proprietà intellettuale e tutelando la privacy degli utenti.
Le tecnologie avanzate (Wiafe et al. 2020) di Machine Learning (ML) e Intelligenza Artificiale (AI) stanno inoltre trasformando le strategie di sicurezza. Questi strumenti permettono alle biblioteche di anticipare, rilevare e rispondere alle minacce in tempo reale, migliorando significativamente la capacità di adattarsi a un panorama di minacce in continua evoluzione.
Infine, la tecnologia Blockchain offre nuove opportunità per garantire la sicurezza e l'integrità delle collezioni digitali. Grazie alla sua natura decentralizzata e immutabile, Blockchain può essere utilizzata per autenticare documenti, mantenere percorsi di controllo a prova di manomissione e preservare l'autenticità di dati storici, risultati di ricerca e proprietà intellettuale. Questa tecnologia si dimostra particolarmente utile nella conservazione di lungo termine e nella verifica dell'autenticità dei materiali delle biblioteche digitali.
Combinando queste soluzioni tecnologiche, le biblioteche digitali possono costruire un'infrastruttura di sicurezza robusta e resiliente, capace di rispondere alle esigenze del presente e prepararsi alle sfide future.

6. Iniziative in corso

L'attenzione per la sicurezza informatica degli oggetti digitali culturali sta emergendo a livello internazionale, ma primariamente in Italia con iniziative recenti di ampio respiro (Gatti 2024, Pasqui 2021). La nascita del Working Group su Cyber Humanities presso il Consorzio Interuniversitario Nazionale per l'Informatica (CINI) al quale hanno aderito più di 34 università e centri di ricerca italiani, la costituzione di un Technical Committee[7] e della relativa conferenza internazionale[8] sempre su Cyber Humanities presso l'Institute of Electrical and Electronics Engineers (IEEE), oppure l'istituzione del primo corso di alta formazione in Cyber Humanities and Heritage Security[9] presso l'Università di Roma Tre vanno in questa direzione. E non è un ca-

[7] https://www.ieeesmc.org/technical-activities/cybernetics/cyber-humanities/.
[8] https://www.ieee-ch.org/.
[9] https://studiumanistici.uniroma3.it/didattica/post-lauream/chhs/.

so che questa sensibilità sia emersa proprio in Italia, dove c'è una diffusa competenza sul digitale per i beni culturali che ci ha consentito di essere in prima fila nelle campagne di digitalizzazione per la creazione di Europeana[10] (la biblioteca digitale europea), così come in quelle relative alla conservazione di lungo periodo (vedi i progetti Magazzini Digitali per la conservazione delle risorse digitali culturali e il National Bibliography Number - NBN:IT per la loro identificazione affidabile, con una storia di ricerca e sviluppo di già 15 anni presso la Biblioteca Nazionale Centrale di Firenze). Anche se tali competenze non erano immediatamente riconducibili alla sicurezza informatica propriamente detta, temi come la preservazione inalterata dei bitstream, il problema della certificazione della provenienza e della catena di custodia delle risorse digitali, così come quella dell'autenticità o del tracciamento delle modifiche, hanno oggi piena cittadinanza nel dominio della sicurezza informatica, considerata ormai un concetto olistico nel quale si fanno ricadere sempre più aspetti. Questa tendenza consente di declinare i requisiti di conservazione e sicurezza degli oggetti culturali digitali gestiti dalle biblioteche digitali beneficiando di innovazioni tecnologiche, concetti e standard già utilizzati in altri settori considerati ad oggi maggiormente a rischio.

7. Conclusioni

Le biblioteche digitali sono risorse con valore inestimabile nel panorama accademico e pubblico, ma la loro sicurezza è costantemente messa alla prova dalle minacce informatiche (Bellini – Tammaro 2024).

Le strategie di cybersecurity delineate devono essere integrate in modo organico nella governance delle biblioteche digitali, rappresentando un pilastro essenziale per il loro funzionamento. L'implementazione di queste misure, tuttavia, richiede risorse consistenti e una stretta collaborazione tra esperti di Information Technology (IT), amministratori di biblioteca, bibliotecari e altre parti interessate. Questo evidenzia la necessità di un approccio transdisciplinare, in cui competenze diverse si intrecciano per affrontare in modo sistemico le sfide della sicurezza informatica.

Le biblioteche digitali, infatti, non possono limitarsi a reagire alle minacce, ma devono adottare un approccio proattivo che consenta di anticipare e mitigare i rischi. In questo contesto, l'applicazione della prospettiva delle infrastrutture critiche offre un modello efficace per perseguire obiettivi di resilienza. Tale approccio non si limita alla protezione delle risorse e al mantenimento della fiducia degli utenti, ma sottolinea il ruolo delle biblioteche digitali come servizio essenziale per la società, capace di continuare a operare e a garantire l'accesso alla conoscenza anche in situazioni di crisi.

Investire nella cybersecurity e nella cyber resilience non è solo una questione tecnica, ma rappresenta una salvaguardia della missione fondamentale delle biblioteche digitali: preservare e diffondere la conoscenza. Un approccio transdisciplinare è, in questo senso, cruciale per integrare competenze tecnologiche, gestionali e culturali, creando soluzioni innovative che possano rispondere alle esigenze complesse di un ambiente umano-cyber-fisico sempre più interconnesso.

[10] https://www.europeana.eu/it.

Understanding cybersecurity in the Cultural Heritage domain and addressing the evolving threats to digital libraries has become an imperative for their sustainability and reliability. This article explores the complex landscape of digital library cybersecurity, identifying key challenges and vulnerabilities while presenting strategies to protect digital repositories and safeguard user privacy. Special attention is given to the pivotal role of cybersecurity-aware librarians, who not only implement protective measures but also educate users and empower communities to engage confidently with digital library resources in an increasingly interconnected and vulnerable digital ecosystem.

L'ultima consultazione dei siti web è avvenuta nel mese di dicembre 2024

Riferimenti bibliografici

Adakawa 2022 — Murtala Ismail Adakawa. *Libraries, cybersecurity, and webinars*. «Journal of Information Studies and Technology», (2022), n. 2. <https://doi.org/10.5339/jist.2022.11>.

Anday et al. 2012 — Audrey Anday et al. *Information security issues in a digital library environment: a literature review*. «Bilgi Dünyası», 13 (2012), n. 1, p. 117-137. <https://doi.org/10.15612/BD.2012.171>.

Bellini – Tammaro 2024 — Emanuele Bellini – Anna Maria Tammaro. *Cybersecurity for digital libraries: an interview with Emanuele Bellini*. «Digital Library Perspectives», 40 (2024), n. 2, p. 348-355.

Farid et al. 2023 — Ghulam Farid – Nosheen Fatima Warraich – Sadaf Iftikhar. *Digital information security management policy in academic libraries: A systematic review (2010–2022)*. «Journal of Information Science», (2023). <https://doi.org/10.1177/01655515231160026>.

Fox – El Sherbiny 2011 — Edward Fox – Noha El Sherbiny. *Security and digital libraries*. In: *Digital Libraries-Methods and Applications,* ed. by Kuo-Hung Huang. InTech, 2011, p. 151-160. <https://www.intechopen.com/chapters/14701>.

Gatti 2024 — Andrea Gatti. *Cybersicurezza e privacy: le sfide per la società e il diritto*. In: *Riflessioni in biblioteca*, a cura di G. Manica. Firenze: Polistampa, 2024, p. 97-113.

Han et al. 2016 — Zhengbiao Han et al. *Risk assessment of digital library information security: a case study*. «The electronic library», 34 (2016), n. 3, p. 471-487. <https://doi.org/10.1108/EL-09-2014-0158>.

Huang et al. 2019 — Shuiqing Huang et al. *Factor identification and computation in the assessment of information security risks for digital libraries*. «Journal of Librarianship and Information Science», 51 (2019), n. 1, p. 78-94. <https://doi.org/10.1177/09610006166685>.

Kuzma 2010 — Joanne Kuzma. *European digital libraries: web security vulnerabilities*. «Library Hi Tech», 28 (2010), n. 3, p 402-413. <https://doi.org/10.1108/07378831011076657>.

ISO 27000 2018 — ISO/IEC 27000:2018. *Information technology - Security techniques - Information security management systems - Overview and vocabulary*. <https://www.iso.org/obp/ui#iso:std:iso-iec:27000:ed-5:v1:en>.

Kim 2016 — Bohyun Kim. *Cybersecurity and digital surveillance versus usability and privacy: why libraries need to advocate for online privacy*. «College & Research Libraries News», 77 (2016), n. 9, p. 442-451. <https://doi.org/10.5860/crln.77.9.9553>.

Kont 2024 — Kate-Riin Kont. *Libraries and cyber security: the importance of the human factor in preventing cyber attacks*. «Library Hi Tech News», 41 (2024), n. 1, p. 11-15. <https://doi.org/10.1108/LHTN-03-2023-0036>.

Ngwum et al. 2020 — Nnatubemugo Innocent Ngwum et al. *Security Evaluation of Digital Libraries*. AMCIS. Americas Conference on Information Systems, 2020. <https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/24/>.

Pasqui 2021 — Valdo Pasqui. *Biblioteche digitali e trasformazione digitale della PA*. «Dig*Italia*. Rivista del digitale nei beni culturali», 16 (2021), n. 1, p. 9-37. <https://doi.org/10.36181/digitalia-00024>.

Wiafe et al. 2020 — Isaac Wiafe – Felix Nti Koranteng – Emmanuel Nyarko Obeng – Nana Assyne – Abigail Wiafe – Stephen R. Gulliver. *Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature*. «IEEE Access», 8 (2020), p. 146598-146612. <https://ieeexplore.ieee.org/document/9152956>.

Yin 2024 — Yimin Yin. *Information Security and Risk Control Model Based on Plan-Do-Check-Action for Digital Libraries*. «Journal of Cyber Security and Mobility», 13 (2024), n. 2, p. 305-326.