International Federation of Library Associations and Institutions

Соопштение на ИФЛА за сајбер-безбедноста

одобрена од Управниот одбор на ИФЛА, февруари 2022

Ова соопштение за политиката на ИФЛА, чија цел се библиотеките, библиотекарските здруженија и библиотекарските едукатори, како и владите (вклучувајќи ги и меѓувладините организации), се обидува да го објасни концептот на сајбер-безбедноста во контекст на работата на библиотеките и да изработи препораки за подобрување.

Библиотеките претставуваат почетен провајдер (обезбедувач) на информации, а особено јавните библиотеки имаат сè поголема улога во израмнувањето на нееднаквоста во пристапот до информациите. При спроведување на оваа мисија, библиотеките сè повеќе се потпираат на дигиталните технологии, подеднакво и при обезбедувањето пристап до информациите, како и при обезбедување ефективно сопствено работење.

Правејќи го ова, тие се соочуваат со фактот дека ваквите системи можат да бидат подложни на напади, изложувајќи ги на ризик институциите, вработените и корисниците. Сајбер безбедноста е исто така важен елемент во работата на библиотеките, чија цел е да ги заштити и корисниците на библиотеката и вработените додека обезбедува пристап до информации за поширокаата јавност.

Исто така, постои зголемена потреба да се разгледа како библиотеките ќе им пристапуваат на прашањата за сајбер-безбедноста, на начин на кој ќе ги поддржува клучните вредности поврзани со интелектуалната слобода.[1]

Сајбер-безбедност, и зошто е важна за библиотеките

Дефиницијата за сајбер-безбедност се фокусира на заштитата на мрежите, опремата и податоците од неавторизиран пристап и/или користење. Непосредно поврзано со ова се напорите да се обезбеди доверливост, интегритет и достапност на информациите.[2] Други пак го

1 Ова вклучува слобода на искажување мислење без мешање и слобода на барање, примање и пренесување на информации и идеи преку кој било медиум без (разлика на) ограничувања (вклучувајќи ја слободата за читање, и пошироко, слободата за пристап до информации и слободата за изразување). Да се види Соопштението на ИФЛА за приватноста во библиотекарската околина (2014): https://www.ifla.org/wp-content/uploads/2019/05/assets/hgnews/documents/ifla-statement-on-privacy-in-the-library-environment.pdf, и Соопштение за библиотеките и интелектуалната слобода (1999): https://repository.ifla.org/handle/123456789/1424

2 Да се види Агенцијата на САД за сајбер безбедност и инфраструктурна безбедност https://us-cert.cisa.gov/ncas/tips/ST04-001, Националниот центар за сајбер-безбедност: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security, ENISA: https:/www.enisa.europa.eu/publications/definition-of-cybersecurity.

сместуваат во рамки на поширокиот концепт на Дигиталната безбедност, која ги надминува техничките и/или криминалните со цел исто така да ги опфати економските и социјалните аспекти.[3]

Стандардите за центарот за сајбер-безбедност за компонентите на информацискиот систем:

- критични апликации
- сервери и инсталации што ги поддржуваат апликациите (центри за податоци итн.)
- безбедност околу мрежите што ги поддржуваат системите
- безбедноста околу развојот на софтверот, контрола над измените и распоредувањето
- крајниот корисник или средината на клиентот

Овие стандарди се релевантни за библиотеките во нивните напори да овозможат сајбер-безбедност иако сите библиотеки го немаат истото ниво на контрола над различните компоненти во системите што ги користат. Сместени во многу различни институционални контексти, политиките за сајбер-безбедност на библиотеката често ќе зависат од сеопфатните политики на владините институции.

На пример, библиотеките можат да имаат ограничено влијание во управувањето со инфраструктурата врз основа на која функционираат, но се обично инволвирани во средината на крајниот корисник или клиент, и имаат критична улога во селекцијата, администрацијата, образованието или менаџирањето на библиотечните системи и давањето на услуги.

Области за ангажирање на библиотеките или застапување (застапништво)

Без оглед дали е тоа преку нивните постапки или преку влијаење врз постапките на другите, библиотеките би требало да ја промовираат сајбербезбедноста во следниве области:

(1) заштита на библиотечните системи од ризици и закани по сајбербезбедност со цел да овозможи тековно обезбедување на услугите;
(2) обезбедување на заштита на корисниците на библиотеките од заканите што доаѓаат од интернет додека ги користат библиотечните системи;
(3) заштита на приватноста на информациите на корисниците.

Многу библиотеки, во обезбедувањето пристап до интернет, исто така ќе имаат законска или друг вид обврска да се осигурат дека пристапот не се употребува за да наштети некому. Исто така, библиотеките можеби ќе треба да преземат чекори за да се осигураат дека и самите корисници не преземаат сајбер-криминални активности користејќи ги библиотечните системи или ресурси и дека ги почитуваат правилата за користење на услугите на институцијата.

Уште попозитивно, со оглед на тоа дека корисниците можат да го користат интернетот и другите информациски системи надвор од библиотеката, исто така постои можност да се промовираат однесувања и протоколи за безбедно користење на услугите преку програмите за дигитална писменост.[4]

---

3 OECD: https://www.oecd.org/digital/ieconomy/digital-security

4 На пример, Стратегијата за безбедноста на Интернет на Обединетото Кралство ја нагласува важноста на образованието: https>//www.gov.uk/government/consultations/internet-safety-strategy-strategy-green-paper

Да се постигне рамнотежа

Промовирањето на сајбер-безбедноста секако дека не е неконтроверзно. Напорите да се идентификуваат потенцијалните ризици може исто така да дојдат во конфликт со напорите да се осигура приватноста на корисниците на библиотеката и на другите.

На пример, библиотеките можат да се обврзат да имплементираат технологии со кои ќе се спроведуваат политики за дозволено користење или да подлежат – заедно со корисниците на интернет воопшто – да бидат под надзор на безбедносните органи. Во вакви случаи, важно е да се биде транспарентен во врска со правилата и алатките што се користат со цел да им се даде разумен избор на корисниците.

Секако, од друга страна, целите на стратегиите за сајбер-безбедност и приватност можат да се вклопат заедно. На пример, ризикот за губење на лични податоци преку сајбер-напади може да биде минимизиран ако, прво, библиотеките не чуваат непотребни лични податоци и второ, да се сигурни дека тие податоци се прописно шифрирани (заштитени).

Препораки

Затоа, ИФЛА ги дава следниве препораки.
Без разлика дали имаат (целосна или делумна) одговорност за нивните информатички системи, библиотеките, треба:

- Да имплементираат политики на минимизирање на собирање и задржување податоци, вклучувајќи и бришење на историјата на користење по одреден дефиниран временски период.
- Да користат достапни алатки да ги заштитат корисниците додека тие ги користат библиотечните системи, вклучувајќи стандардни мерки за информациска безбедност, како што се шифрирани веб-услуги, ефективни лозинки и контроли на веб-сесиите, или примена на принципите на најмала привилегија[5], обезбедувајќи во исто време максимална приватност.
- Да имплементираат безбедосни контроли за крајниот терминал на сите библиотечни работни станици и сервери[6].
- Да определат каде ќе бидат имплементирани алатките за мониторирање на несоодветното користење или ненамерни закани, па да го направат тоа на начин кој обезбедува максимална транспарентност и почитување на приватноста.

Онаму каде што се дел од поголема институција (и заради тоа, немаат контрола над клучните компоненти на информациските системи) или зависат од надворешни доставувачи:

---

5 https://en.wikipedia.org/wiki/Principle of least privilege

6 Бројни ИСО стандарди ги покриваат прашањата околу сајбер-безбедноста. Како и да е, овие стандарди се недостапни пеку слободен пристап и не можат да бидат одборени од ИФЛА како модели за глобалната библиотечна област. Примерите ги вклучуваат ИСО 27001 – Систем за управување со безбедност на информациите – Барања (Information Security Management System - Requirements), www.iso.org/isoiec-27001-information-security.html; ИСО 270002 - Код за практикување на управувањето со безбедноста на информациите (Code of Practice for Information Security Management), https;//www.iso.org/standard/54533.html; ИСО 27032 – Информациска технологија – Безбедносни техники – Водич за сајбер-безбедност (Information technology – Security techniques – Gudilenes for cybersecurity), https://www.iso.org./standard/44375.html

- Да се залагаат за ефективни сајбер-безбедносни мерки од страна на надлежните институции, кои исто така ги поддржуваат принципите за приватност. Ова исто така вклучува промовирање на практиките за зачувување на приватноста особено околу собирањето и задржувањето на податоците.
- Да се охрабрат надворешните доставувачи, чии услуги ги користат библиотеките, да имплементираат и самите значајна сајбер-безбедност, со цел да обезбедат дека корисниците на библиотеките нема да се соочат со ниеден неприфатлив ризик кога ќе ги користат нивните услуги.

Сите библиотеки треба:

- Без разлика дали сами или во партнерство со надлежната институција (host institution), како што е соодветно:
  - да развиваат и да објавуваат политики за дозволено користење на интернет и за користењето на другите информациски системи.
  - Да развиваат и да објавуваат политики за приватност, дефинирајќи каде и која информација е собрана и како ќе биде употребена, и што ќе се случи во случај на прекршување.
  - Да развиваат и да објавуваат политика за сајбер-безбедност и за информациска безбедност која ги дефинира принципите и практиките користени за заштита на библиотечните системи и да обезбедат отпорност и закрепнување во случај на пад на системите. Ова треба да е усогласено со институционалните политики и процедури за оваа област.
  - Да се осигурат дека сите вработени во библиотеката ги разбрале и се способни да ги применуваат основите на сајбер-безбедноста (на пример, добри практики за лозинки) релевантни за нивните работни обврски.
- Да го истражат потенцијалот за градење на дигитална писменост помеѓу корисниците, вклучувајќи го разбирањето за тоа како да се избегнат заканите по сајбер-безбедноста.

Библиотекарските здруженија и другите поддржувачки организации треба:

- Да обезбедат соодветни ажурирања и информации за сајбер-безбедност во работата на библиотеките и, таму каде што е можно, да понудат обуки или линкови до други извори.
- Да се разгледа работењето со други страни кои се ангажирани во помагањето на луѓето да бидат безбедни додека се онлајн.

Властите треба:

- На библиотеките да им обезбедат ресурси и обуки за да бидат способни да ја максимизираат сајбер-безбедноста, како и да инвестираат во програми за дигитална писменост (и преку библиотеките) со цел да ја промовираат онлајн-безбедноста.
- Да се погрижат општите политики за сајбер-безбедност да ја спојат ефективноста со почитувањето на човековите права, вклучувајќи ја приватноста.

Анекс: ИСО стандарди

ИСО стандардите обезбедуваат општ пакет на стандради за сајбер- и информациска безбедност во која било организација. Ова треба да ја формира основната линија за практиките за Информацискатa технологија во однос на техничките аспекти на сајбер-безбедноста во библиотеката.

ИСО/ИЕЦ 27001 – Систем за управување со безбедност на информациите – Критериуми (Information Security Management System – Requirements) ги специфицира критериумите за добро дефиниран Систем за управување со безбедноста на информациите (СУБИ) внатре во организацијата. Ова ги опфаќа систематските процеси за безбедносно управување.[7]

ИСО/ИЕЦ 27002 Код за практикување на управувањето со безбедноста на информациите (Code of Practice for Information Security Management) содржи насоки и препораки од најдобрите практики за 10 клучни безбедносни полиња: безбедносна политика; организација на безбедноста на информациите; управување со средства; безбедност на човечките ресурси; физичка безбедност и безбедност на околината; комуникациско и оперативно управување; контрола на пристап; набавка, развој и одржување на информациски ситеми; управување со инциденти во информацискатa безбедност; управување со континуитет на деловното работење; и усогласеност. Ова е типично во доменот на управувањето на информациските системи со архитектурата на информацискатa технологија.[8]

ИСО 27032 – Информациска технологија – Безбедносни техники – Водич за сајбер-безбедност (Information technology – Security techniques – Gudilenes for cybersecurity)

ИСО/ИЕЦ 27002 Код за практикување на управувањето со безбедноста на информациите (Code of Practice for Information Security Management) се проширува на основната линија на практиките за сајбер-безбедност.[9]

https://www.iso.org./standard/44375.html

7 https://www.iso.org/standard/5434.html
8 https://www.iso.org/standard/54533.html
9 https://www.iso.org./standard/44375.html