Skydd för personlig integritet i biblioteksmiljö

Checklista v 0.1

National Library of Sweden

Biblioteken i det allmänna biblioteksväsendet ska verka för det demokratiska samhällets utveckling genom att bidra till kunskapsförmedling och fri åsiktsbildning. Det innebär att tillgång till internet är en viktig tjänst att tillhandahålla besökarna på ett bibliotek. Det innebär dock inte att besökare ska kunna göra vad de vill med bibliotekets utrustning eller få tillgång till andra besökares information. Biblioteksanvändare måste kunna ha förtroende för att deras användning av bibliotekets tjänster inte innebär intrång i den personliga integriteten genom att andra får åtkomst till känslig information.

Detta dokument är en första checklista med syfte att minska risken för intrång i besökarnas personliga integritet när de använder digitala tjänster i biblioteksmiljö. Checklistan är inte heltäckande för alla typer av tjänster och områden. Tanken är att du som använder checklistan ska få ett underlag för att föra ett resonemang med kollegor och leverantörer om hur ni kan minska risken för intrång i besökarnas personliga integritet.

Checklistan är indelad i tre delar:

A. Fysisk åtkomst – hur du kontrollerar och förhindrar åtkomst till datorer för att undvika att besökare installerar utrustning som kan användas för att komma åt andra användares information.

B. Konfiguration av datormiljö – grundläggande krav på nedlåsning av datormiljön för att undvika skadlig kod.

C. Bibliotekets tjänster på webben – hur du undviker att dela med dig information om dina besökares aktiviteter till obehöriga.

För varje del bör du dokumentera utfallet och sedan planera möjliga åtgärder med din it-leverantör. Om möjligt bör du genomföra testet tillsammans med någon från din it-organisation.

A. Fysisk säkerhet

A1. Undvik att ha kontakter för datorer och kringutrustning åtkomliga för besökarna

Om en användare kan komma åt kontakterna till t.ex. tangentbordet finns det risk för att någon kopplar in loggningsutrustning som kan fånga upp andra besökares tangentbordsaktivitet (key logger). På detta sätt kan en illvillig användare komma över lösenord, innehåll i e-post och annan information som besökarna skriver in via datorns tangentbord.

Hur du kontrollerar

Kontrollera att kablage är inlåst, inkapslat eller på annat sätt har gjorts oåtkomligt för besökare. Går det att koppla ur tangentbordet och koppla in något mellan tangentbordssladden och datorn? Går det att komma åt nätverkskontakter?

Förslag på åtgärder

- Kontakta din it-leverantör för att diskutera möjliga lösningar för inlåsning av kablage och utrustning. Det finns tillbehör till många datormodeller där kablage och dator kan låsas in.
- Om kablaget inte är inlåst behöver du göra regelbundna inspektioner av utrustningen för att se att inte någon kopplat in obehörig utrustning som t.ex. en keylogger.

A2. Minimera ”över-axeln”-åtkomst till information

I den publika miljön kan det vara svårt att använda datorn för känslig information om det sitter andra personer som ser skärmen i närheten. Försök att placera skärmar och sittplatser på ett sätt som minimerar risken för insyn. Detta gäller även utskriftshantering. Kan andra få tillgång till utskrifter som en annan användare har startat?

Hur du kontrollerar

- Testa om det går att se skärmen från andra sittplatser i närheten av terminalerna. Kan man se vad någon surfar på för webbplatser?
- Vid utskrift, finns det risk för att utskrifter ligger synliga för andra? Går det att slänga utskrifter på ett sätt som inte ger andra tillgång till informationen, t.ex. i en låst papperskorg?

Förslag på åtgärder

- Placera skärmar direkt på skrivbordet istället för ovanpå datorn om möjligt. En lägre placerad skärm gör det svårare för andra som sitter bakom att se skärmens innehåll.
- Överväg möjligheterna att utrusta skärmarna med sekretessfilter (en plastfilm som minimerar insyn från sidan av skärmen).
- Överväg möjligheten att ställa ut låsbart återvinningskärl för papper.

A3. Försvåra avlyssning av nätverket i lokalerna

Om besökare kommer åt att koppla in egen utrustning i nätverksuttag behöver du minimera risken för att de får tillgång till andras information.

Hur du kontrollerar

- Testa att koppla in en dator som inte hör till din organisation i ett nätverksuttag i lokalerna. Vilka tjänster kommer man åt? Kan man se andra datorer i nätverket?
- Om ditt bibliotek har trådlöst internet för besökarnas egna datorer, kontrollera att krypteringen har aktiverats (minst wpa-2).
- standardlösenordet för administratörer är bytt
- ssid är ändrat
- dhcp-adresseringen har begränsats (max antal samtidiga användare)
- wan-förfrågningar har blockerats (icmp ping blocked)
- externa administrationen är avstängd (kräver sladd till routern)

Förslag på åtgärder

Kontakta din it-leverantör för att gå igenom möjliga åtgärder för att skapa en säkrare nätmiljö i lokalerna.

B. Konfiguration av mjukvarumiljö

B1. Minimera risken att information från tidigare användare är tillgänglig

Efter att en användare lämnar en terminal är det viktigt att den information som användaren lämnar efter sig inte blir tillgänglig för andra användare. Det gäller tillfälliga dokument som kanske sparats på datorn, inloggningar i olika tjänster, surfhistorik, utskrifter som fastnat i skrivarkön med mera.

Hur du kontrollerar

Genomför en användningssession på samma sätt som en vanlig besökare gör. Notera vilka webbadresser du besöker, mata in information i formulär och skicka in dem, spara filer på skrivbordet och så vidare. Avsluta sessionen enligt de instruktioner som finns och gå in som en ny användare.

- Finns dokument kvar på skrivbordet eller i tillfälliga filer?
- Kan man se surfhistorik i webbläsaren?
- Har kakor sparats?
- Har formulärinformation sparats?
- Kan man se vilka dokument som nyligen öppnats i olika program på datorn?
- Skriv ut ett dokument till en avstängd skrivare. Om användaren lämnar datorn och skrivaren senare slås på, kommer dokumentet skrivas ut ändå?

Förslag på åtgärder

Nedlåsning av de publika terminalerna kan behöva ske på flera olika sätt beroende på programvara, datormiljö mm. Gå igenom resultatet av kontrollen med din it-leverantör och undersök hur brister kan åtgärdas.

B2. Låt inte användare installera egen programvara eller komma åt systemkataloger

Om användare kan installera egen programvara på bibliotekets datorer finns risk för att sådan programvara fångar upp efterföljande användares information. Konfigurera miljön så att programvara inte kan installeras av obehöriga. Dölj och blockera tillgång till operativsystemsfiler/kataloger så att vanliga användare inte kan byta ut filer där.

Begränsa vanliga användares behörigheter till ett minimum. Inga admininstratörsrättigheter ska finnas kvar (installera och exekvera program, göra uppdateringar, ta bort program etc.).

Hur du kontrollerar

- Använd datorn såsom en biblioteksbesökare skulle göra. Försök att installera ett program på datorn genom att ladda ner installationsfiler för t.ex. *Firefox* eller någon annan fri programvara som inte redan finns på datorn. Kör installationsprogrammet. Gick det att installera? Om det gick att installera programvaran, finns den kvar när nästa användare använder datorn (se B1 ovan).
- Försök öppna en katalog som hör till operativsystemet. Går det att spara filer i där?
- Går det att installera tillägg i webbläsaren på ett sätt så att tilläggen finns kvar när nästa besökare använder datorn?

Förslag på åtgärder

Kontakta din it-leverantör och be dem låsa ned it-miljön så att obehöriga inte kan installera programvara eller komma åt operativsystemets filer.

B3. Skydda användare från skadlig kod

Användare kan behöva ladda ner dokument från nätet. Minimera risken för att de drabbas av virus eller sprider vidare smittade filer genom att tillhandahålla en antiviruslösning på datorerna. Även om inte bibliotekets dator påverkas permanent kan användaren bidra till att smittade filer sprids vidare om det saknas antiviruslösning på datorn.

Hur du kontrollerar

- Finns det antivirusprogram på datorn?
- Är konfigurationsfilerna aktuella? Kontrollera datum då de senast uppdaterades i antivirusprogrammet. Vanligen uppdateras de varje dag.

Förslag på åtgärder

Om antivirus saknas, beställ installation av antivirus på bibliotekets terminaler och säkerställ att konfigurationen uppdateras automatiskt och kontinuerligt.

B4. Minimera åtkomst till loggar

Även om bibliotekets publika datorer klarar övriga checklistepunkter bör du säkerställa att information om dina besökare inte sprids vidare till tredje part. Om din organisation använder produkter som loggar nätverkstrafik bör du säkerställa att det finns rutiner för vem som har tillgång till information i loggarna.

Hur du kontrollerar

Kontakta din it-leverantör för att höra om loggning av användarna sker och vilka rutiner det i så fall finns för åtkomst till loggarna.

Förslag på åtgärder

Be din it-leverantör att upprätta riktlinjer för vem som har tillgång till loggar och i vilka situationer tillgång ges.

C. Bibliotekets tjänster på webben

C1. Minimera spridningen av information om användarna till tredje part

Tillhandahållandet av digitala bibliotekstjänster involverar vanligen flera olika aktörer. När bibliotekets tjänster på nätet används finns det risk för att känslig information sprids till andra (t.ex. sökhistorik, besökta länkar mm). Genom att konfigurera de digitala tjänsterna på rätt sätt kan denna spridning minimeras.

Hur du kontrollerar

Det finns flera verktyg för att ta reda på hur information delas med andra. Använd något av verktygen nedan för att testa t.ex. ditt biblioteks webbplats.

Dataskydds verktyg Webbkoll:
https://webbkoll.dataskydd.net/sv

Se även testverktygen:
Ghostery som tillägg till din webbläsare:
https://www.ghostery.com/our-solutions/ghostery-browser-extension

Disconnect https://disconnect.me

Åtgärder

Utfall

PRODUKTION: KUNGLIGA BIBLIOTEKET OKTOBER 2017