imCodes säkerhetsarbete

imCode
Öppna bibliotekslösningar

Presentation

Vilka är vi?

- Totalt 17 anställda.
- Koha sedan 2016
- Representeras idag av: Kalle och Jacob + Crister och Magnus Pettersson

Idag ska vi gå igenom:

- Varför säkerhet?,
- Vad säkerhet är och hur vi arbetar med det (ett par exempel).

Varför säkerhet?

Kravställning:

- Lagkrav: GDPR, PuL, E-privacy (cookies, spårningstekniker etc)
- Interna och externa krav, t ex en särskilt känslig verksamhet

Kvalité och trygghet:

- Konfidentialitet: Information och resurser skyddas från obehörig insyn och åtkomst
- Riktighet: Information är korrekt, uppdaterad, trovärdig
- Tillgänglighet: (Slut)användare kommer åt system. Bibliotek = samhällsviktig institution
- Spårbarhet: Spåra ändringar = Trygghet

Allt mer och ”farligare” attacker:

- Social engineering (AI osv)/Phising
- DDOS
- Intrång (t ex brute force) etc

Ett försvar med flera murar

- Organisation
- Processer
- Ren teknik

… Som hänger ihop. Låt oss se hur!

Organisation

Redundans:

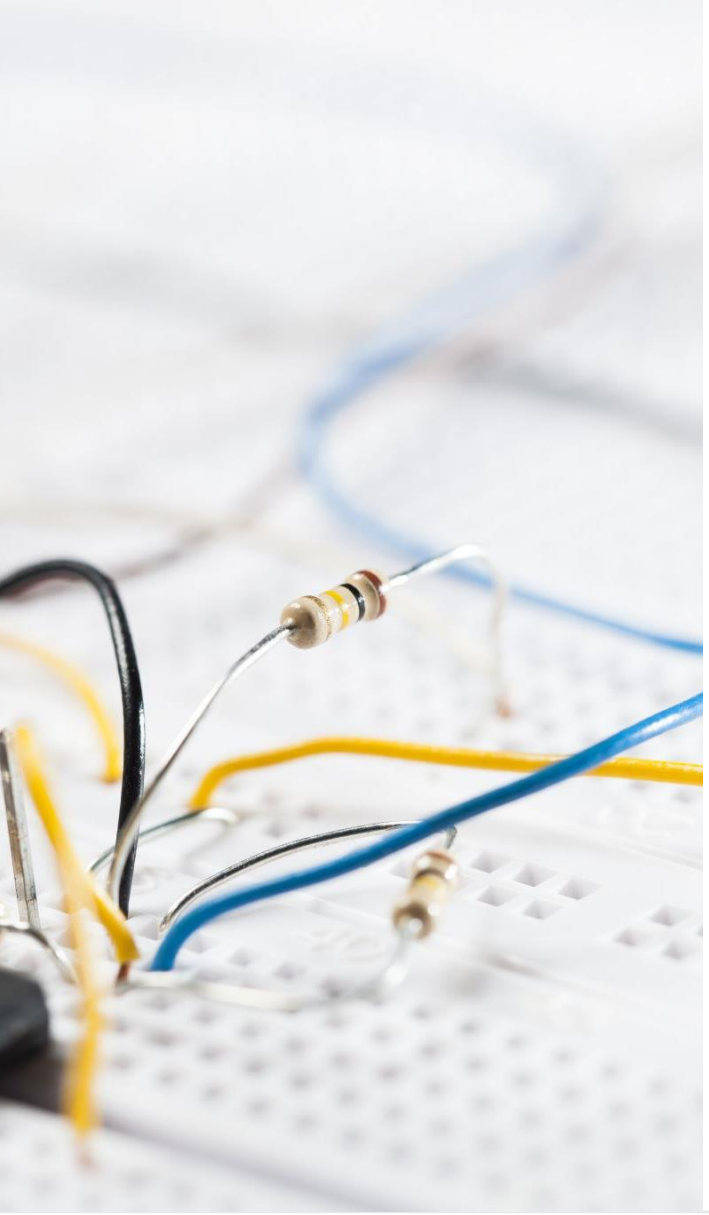
- Sammanlagt 17 personer: 6 bibliotekarier, 3 rena serverteknikker.
- Minst två personer på varje kompetens = Vem som helst kan vara sjuk eller sluta

Rutiner:

- Larm- och supportövervakning dygnet runt.
- Beredskap och jour. Samarbete med support- och kundservicebolag (dygnet runt jour).

Rutiner

- Dokumentation
- Riskanalyser (särskilt vid GDPR åtgärder)
- Eskaleringsrutiner (t ex personuppgiftsincident)
- BitWarden för lösenordshantering
- Ärendehantering för uppföljning, verifiering, återkoppling.
- Patchar (säkerhet)
- Koha-community (bidra med att testa och hitta fel), många kan testa och hitta säkerhetshål.



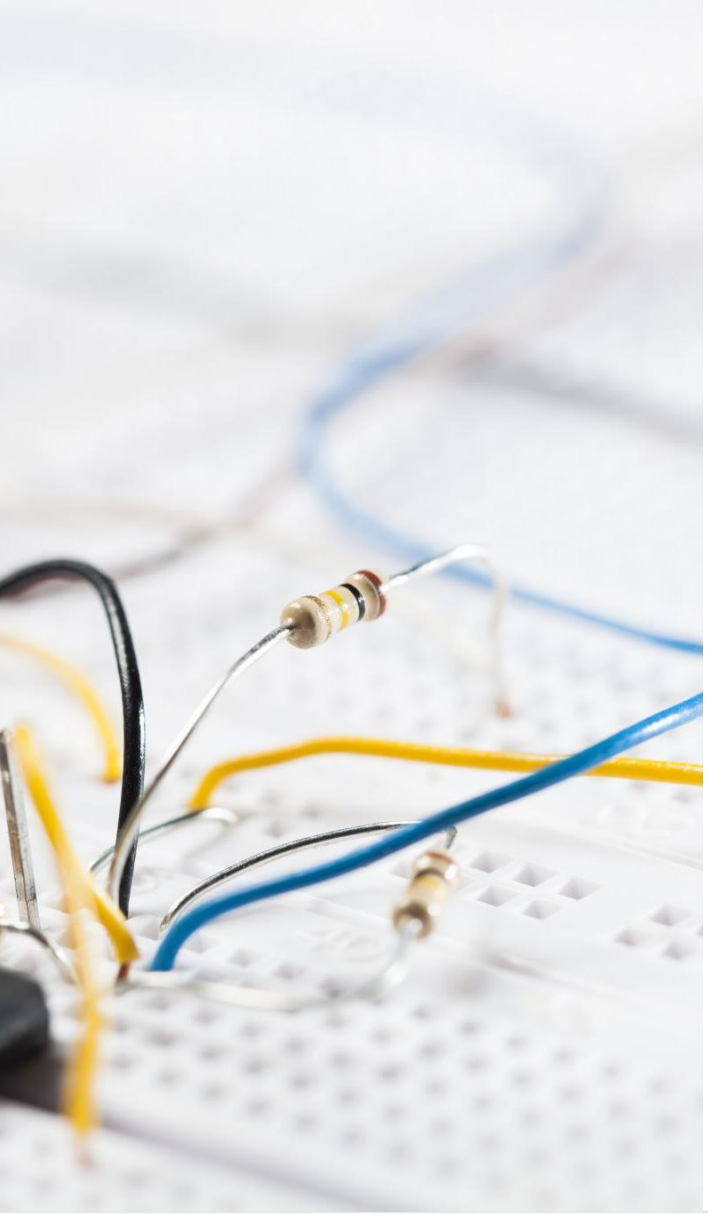
Teknik

Serverhall (Skyddsklass 3):

- Fysisk säkerhet
- Brandsäkerhet
- Strömförsörjning
- Kylsystem
- Nätverkssäkerhet

Säkra data:

- Databas: Master-Slave
- Elastic: Cluster
- Backup: Filer, databas-snapshots mot offsite.
- Config filer: Versionshistorik (2h)
- Github/SVN: Versionshantering



Teknik

Skydd mot intrång:

- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Logganalys
- Honey Pots
- Anomalidetektering

Brandvägg- och nätverkssegmentering

- Databas, webbtjänst etc ligger uppdelat
- En Koha kan ligga helt isolerat

imBlocker idag

- ”DOS- attacker”: Vanligast mot sökningen (t ex opac-search.pl).
- Sökmotorer som inte respekterar robots.txt
- Mycket sökningar utan faktiskt värde (t ex robotar/spindlar)
- Anropssignaturer

imBlocker framåt

- Analys av trafikmängd
- Analys över många webbar
- Analys över lyckade anrop.
- Analys av inloggningsförsök (brute force)
- Analys med AI
- Skydd av mer än bara webbtrafik.
- Automatik av triggers/signaturer/abnormalitet

Att fundera på

- Har vi bra lösenord i personalgränssnittet?
- Hur begränsar vi access till personalgränssnittet?
- Har vi möjlighet att begränsa personalgränssnitt och SIP klienter till vissa IP?
- Jobbar personal hemifrån, och använder de då VPN?

Tack för oss! Frågor?

imCode
Öppna bibliotekslösningar