Informationssäkerhetsberättelse 2018

ANNA-LENA ALFREDS
BEREDSKAPSCHEF

REGION JÄMTLAND HÄRJEDALEN

Informationssäkerhetsarbete 2018

Intensivt år, det dominerande arbetet har varit:

- Anpassning till Dataskyddsförordningen – projekt Garbo
- Office 365 – hanteringsregler m.m.
- Ny lagstiftning – informationssäkerhet för samhällsviktiga och digitala tjänster (NIS direktivet)
- Förstudie avseende behörighetshantering

- Utvecklingen går mot en hårdare kravbild och ökat behov av att rätt åtgärder finns på plats för att skydda vår information
- Teknisk utveckling går framåt i en rasande fart, skapar nya möjligheter
- Verksamheterna har ett högt IT beroende, risker och sårbarheter ökar
- Viten kan dömas med upp till 20 miljoner kronor
- Registrerade kan begära skadestånd

REGION JÄMTLAND HÄRJEDALEN

Dataskyddsförordningen – projekt Garbo

- Anpassning till de nya kraven – arbetet bedrevs i projektform 2017-2018. Projektet avslutades i juni.
- Utökade krav av skydd av personuppgifter (PU), fokus på den registrerades rättigheter
- Organisation för personuppgiftshantering och dataskydd
- Fungerande arbetssätt, utbilda i verksamheten
- Registerförteckning
- Uppbyggnad av regelverk och rutiner
- Förmåga och rutin att incident rapportera till DI (krav inom 72 timmar)
- Förmåga och rutin att lämna ut registerutdrag
- Säkerställa personuppgiftsbiträdesavtal – för samtliga externa parter
- Konsekvensbedömningar för alla PU som innehåller känsliga personuppgifter

REGION JÄMTLAND HÄRJEDALEN

Regionstyrelsen är personuppgiftsansvarig

- RS ska ha ett utsett dataskyddsombud (DSO)
- Organisation införd enligt RS beslut som innebar:

- DSO, 3 biträdande DSO (ett för varje förvaltningsområde), RK inom varje verksamhetsområde/avdelning

- Organisationen haltar – översyn behöver göras under 2019
- Verksamheterna har ett stort behov av stöd i frågor om dataskydd och personuppgiftsbehandling

REGION JÄMTLAND HÄRJEDALEN

Mobila arbetssätt och andelen molntjänster ökar!

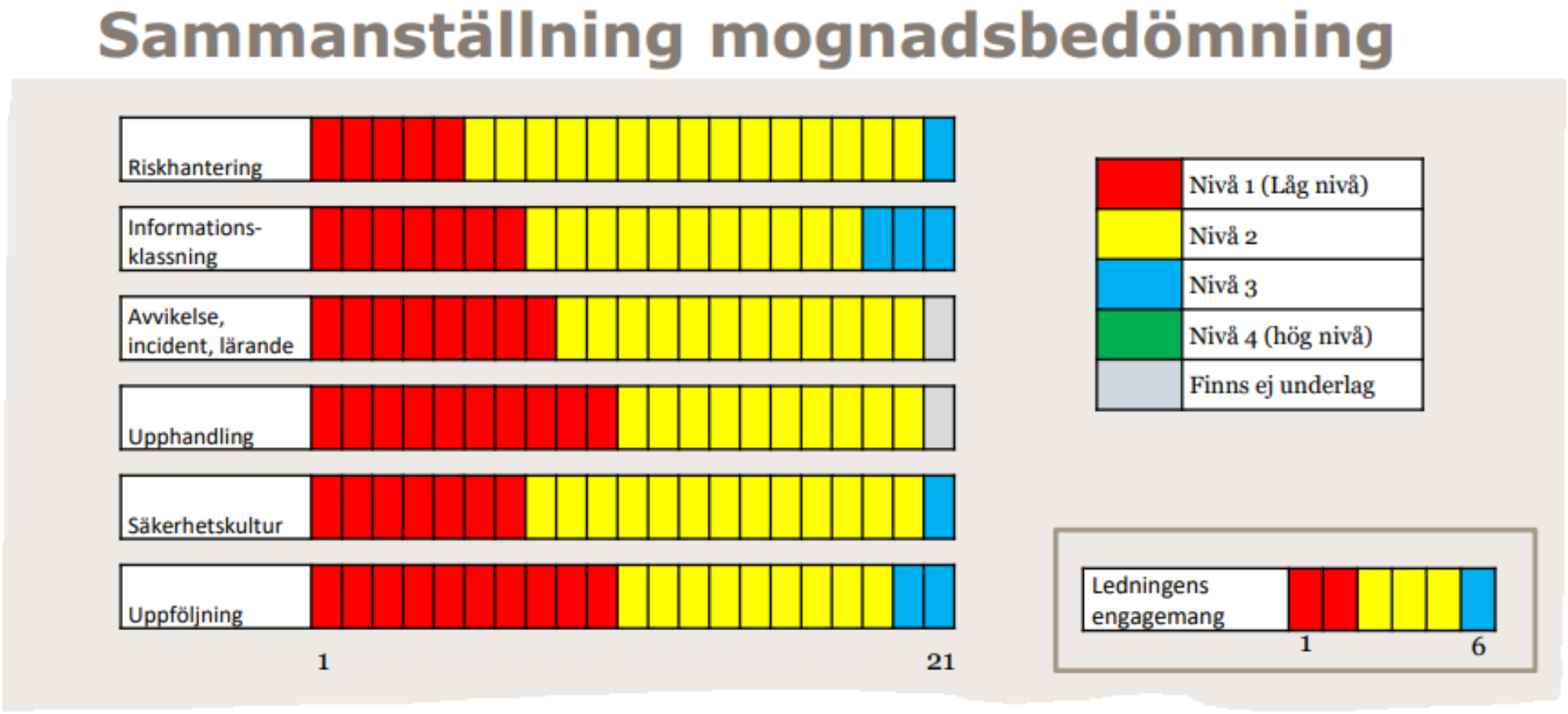
- Säkerheten har svårt att hänga med utvecklingstakten
- Informationsklassning och riskanalys viktiga delar
- Både informations- och IT säkerhetsåtgärder krävs för att användningen ska vara säker
- Vilka uppgifter hanterar vi i mobila verktyg och i molntjänster?
- Den ökade andelen molntjänster kräver att vi ställer om och riktar mer resurser mot kravställning och uppföljning till våra leverantörer

REGION JÄMTLAND HÄRJEDALEN

Nationell rapport om landstingens informationssäkerhetsarbete i hälso- och sjukvården

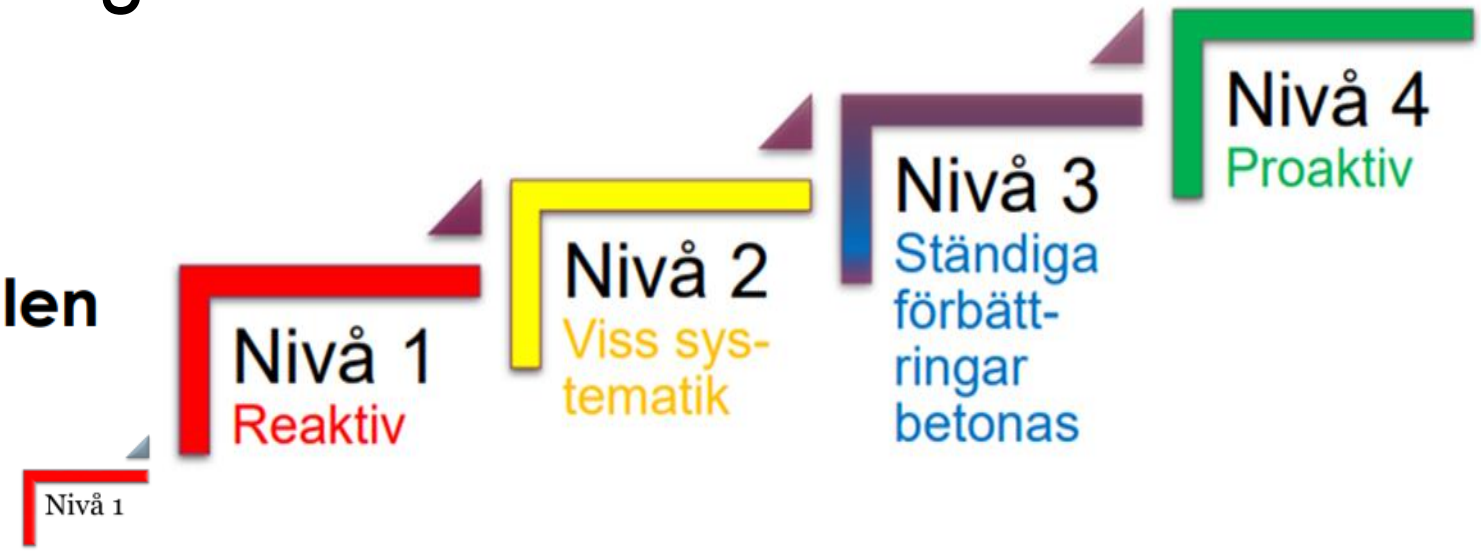
SIQ:s mognadsmodell

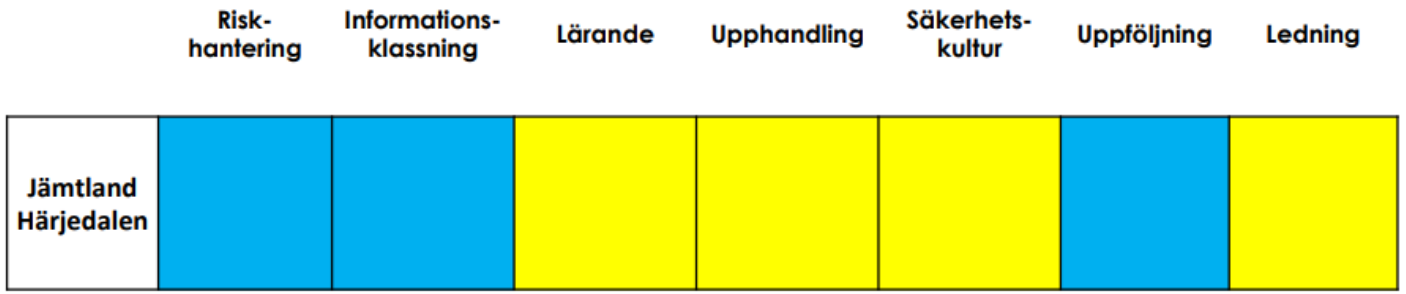
Bedömning alla landsting/regioner



Sammanlagd bedömning

Region Jämtland Härjedalen





REGION
JÄMTLAND
HÄRJEDALEN

Incidenter och avvikelser

- Rapporteras färre avvikelser från verksamheterna
- Tre personuppgiftsincidenter rapporterats till DI (enligt gdpr)
- Sex polisanmälningar om dataintrång (obehörig läsning av journal)

IT attacker, angreppsförsök 2019 – s.k. Brute Force

- Regionen har alltid pågående intrångsförsök från Internet. Dygnet runt, året om.
- Angripare använder en blandning av påhittade och riktiga regionkonton och försöker automatiserat gissa sig till rätt lösenord. Den tjänst som initialt angreps är Office 365.
- Ca 800 av våra konton har förekommit i intrångsförsöken enligt loggarna.
- Under tiden första attacken pågick gjordes över 100 000 misslyckade inloggningsförsök per timme.
- Den stora massan av angrepp kom från maskiner i Ryssland, Kina och Brasilien vid första försöket (vi kan däremot inte säga att angriparna kommer från dessa länder).
- Upptäckt: kontoutlåsningsfunktionen i regionens lösenordspolicy aktiverades per automatik under angreppen och låste ut de ca 150 mest angripna användarkontona
- Kravet om två multifaktorsautentisering för att logga in i Office 365 utanför regionens nätverk hindrar angripare från att logga in även om de lyckas gissa rätt lösenord.

REGION JÄMTLAND HÄRJEDALEN

Hur kan vi drabbas? Varför?

- Hälso- och sjukvårdssektorn överlag drabbade
- Historiskt har HS sektorn inte varit bäst på IT- och informationssäkerhet samtidigt som vi har värdefull information
- Risk som finns – flera tjänster som exponeras mot Internet som inte skyddas av multifaktorsautentisering. En lyckad lösenordsgissning skulle ge tillgång till allt den aktuella användaren har behörighet att göra i tjänsten.
- Om en angripare kommer över användarnamn och lösenord finns flera möjligheter att stjäla information och även att plantera virus – som låser filer och skapar möjlighet till utpressning.
- Patientinformation är ”hårdvaluta”, kan också finnas intressen utifrån Sveriges säkerhet

Hur skyddar vi oss?

- Genomförda åtgärder på kort sikt

- Köpt och aktiverat säkerhetsfunktioner som hjälper till att minska exponeringen för dessa typer av angrepp.

- Förbättrat loggning och spårbarhet.

- scannar hela tiden efter sårbarheter i vår servermiljö. Många sårbarheter upptäcks och kan stoppas.

- Målsättning på längre sikt

- Att samtliga tjänster Region Jämtland Härjedalen exponerar mot Internet skall kräva multifaktorsautentisering vid inloggning.

REGION JÄMTLAND HÄRJEDALEN

Sårbarheter i Heroma

- FRA har utfört penetrationstest av Heroma och hittat sårbarheter de bedömer som kritiska.Ingen information har getts till CGI:s övriga kunder

- Detaljer om sårbarheterna är hemligstämplade av FRA men i media har nämnts möjligheten att göra förändringar i lönekörningar i syfte att förskingra pengar och även risk för läckage av känsliga/skyddade personuppgifter.

- Flertalet regioner har stoppat tillgången till Heroma från Internet för att minska exponeringen. RJH kan inte göra detta då vi numera kör Heroma som molntjänst (sedan 1/3). Tillgången är däremot begränsad till att endast tillåta anslutningar från RJH’s interna nätverk vilket minskar exponeringen så mycket vi kan utan att helt stoppa användandet av Heroma självservice och kom&gå.
- Sårbarheterna finns kvar, men för vår del då från våran driftsmiljö.
- Intern risk - Heroma har inte har tvåfaktors autentisering, inloggning sker med lösenord vilket är ett svagare skydd.

REGION JÄMTLAND HÄRJEDALEN

Prioriterade åtgärder 2019

- Utbildning
- Översyn av organisation Dataskydd
- Kontinuitetshantering verksamhetskritiska IT system vård
- Skyddsfunktioner för känsliga personuppgifter
- Utveckla internkontroll och uppföljning
- Utveckla arbetssätt för informationsklassning och införa nytt verktyg ”Digframe”
- Slutföra förstudie behörighetshantering
- Revidera informationssäkerhetspolicy

- Fortsatt översyn administrativa behörigheter
- Fortsatt insyn sårbarhetsscanning och logganalys
- Riskanalys exponering från leverantörer
- Etablera vitlistningsskydd Citrix
- Analys avseende NIS kraven

REGION JÄMTLAND HÄRJEDALEN

REGION
JÄMTLAND
HÄRJEDALEN