Nyhetsbrev Göliska IT, Nr 2, 2025

Inledning

I det förra nyhetsbrevet beskrev jag bland annat höstens fyra fokusområden för Göliska IT. Ett av dem är att fortsatt stärka IT-säkerheten för att leva upp till kraven från EU:s NIS2-direktiv och den kommande cybersäkerhetslagen. Sammantaget innebär det att vi tillsammans behöver bli bättre på att skydda oss mot cyberattacker. En framgångsfaktor för att lyckas med detta är en ökad samverkan och transparens mellan V6-kommunerna och Göliska IT.

Varje vecka nås vi av nyheter som handlar olika former av cyberrelaterade brott och hot. Under augusti utsattes svenska organisationer för i genomsnitt nästa 1800 cyberattacker i veckan. Majoriteten av attackerna var riktade mot den offentliga sektorn. Det är med bakgrund av detta som regeringens miljardsatsning på nationell cybersäkerhet ska ses. Den syftar till att öka den offentliga sektorns motståndskraft mot cyberattacker och säkerhets incidenter samt att uppfylla kraven från EU:s NIS2-direktiv. (TT intervju med Oskar Bolin 9 september)

Vad avses med begreppet ”cybersäkerhet”?
Begreppet cybersäkerhet, även kallat datasäkerhet, inkluderar även förbyggande, upptäckt och åtgärdande av hot mot IT-infrastruktur, system och information. Med andra ord ett flertal tekniker, processer och metoder som används för att skydda digitala system, nätverk, enheter och data från cyberattacker. Målet är att skydda information från obehörig åtkomst, skada, stöld eller manipulation. Det omfattar allt från att skydda personlig information till att säkra samhällsviktiga funktioner och innefattar både tekniska skydd och organisatoriska rutiner.

Utbildningsdag om NIS2-direktivet och den kommande cybersäkerhetslagen
För att stärka rikets motståndskraft mot cyberattacker och öka datasäkerheten kommer den nya cybersäkerhetslagen att träda i kraft den 15:e januari 2026.

Mot bakgrund av detta har vi inom ramen för samarbetet i V6 starta ett arbete som syftar till att vi gemensamt ska leva upp till den nya cybersäkerhetslagen

Som ett första steg i arbetet bjöd Göliska IT in till en utbildningsdag om den nya cybersäkerhetslagen och dess innebörd för verksamheterna i V6.

Utbildningsdagen syftade till att starta arbetet med följande:

- Sätta standarder för att säkerställa tydliga ansvarsområden och roller för vem som gör vad och när.
- Skapa gemensamma rutiner för säkerhetsarbetet.
- Hur vi strukturerat arbetar tillsammans för att identifiera förbättringsområden.
- Skapa konsensus för hur vi delar nödvändig information mellan medlemskommunerna.

Föreläsningarna kombinerades med gruppdiskussioner vars syfte var att bygga grunden för en tydlig gemensam handlingsplan med målet är att leva upp till de nya säkerhetskraven.

Den nya cybersäkerhetslagen

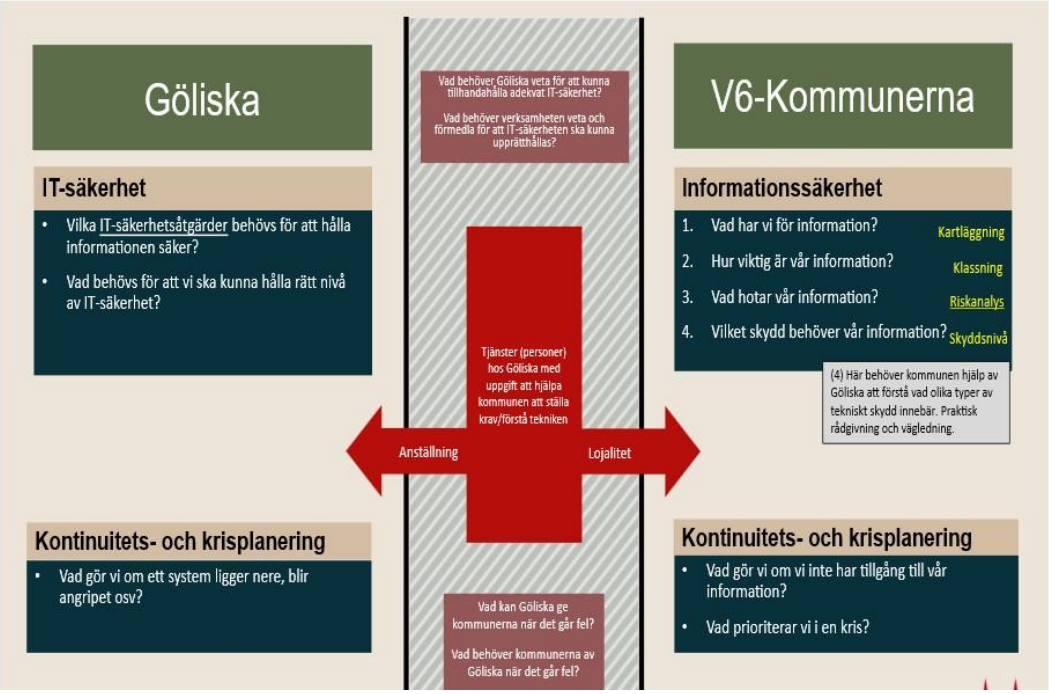
Dagen inleddes av Mikael Hätting, chefsjurist Skara kommun, som utifrån NIS2-direktivet och den kommande cybersäkerhetslagen definierade ett antal hållpunkter. Eftersom V6-kommunerna har lagt ansvaret för sin IT-verksamhet i kommunalförbundet Göliska IT innebär det att Göliska IT har ansvar för V6-kommunernas IT-säkerhet. Kommunerna har ansvaret för informationssäkerheten.

Den kommande lagen anger att verksamhetsutövare ska vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem som de använder för sina verksamheter eller tillhandahåller och systemens fysiska miljö.

Cybersäkerhetslagens 3§ innefattar 10 tydliga punkter som tydligt definierar de områden där vi ska säkerställa säkerheten. Detta inkluderar all verksamhet som är nödvändig och för att skydda nätverks- och informationssäkerhetssystem, användare av dess system och andra berörda personer mot cyberhot.

Mikael beskrev även en modell som tydligt visar de olika ansvarsområden som Göliska IT och kommunerna har för att tillsammans uppfylla de nya kraven.

Föreläsningen avslutades med ett antal områden där vikten av samarbete mellan Göliska IT och V6-kommunerna definierades i syfte att uppfylla de nya kraven. Mikael visade även på den gråzon som kan uppstå mellan Göliska IT om vi inte har tydliga roller och ansvarsområden. Grå-zonen och ansvarsområdena illustreras i bilden nedan.



SKR:s syn på hur cybersäkerhetslagen påverkar arbetets organisation.

På mötet föreläste även Johan Thorén, cybersäkerhetsexpert SKR, om hur cybersäkerhetslagens krav kommer att påverka arbetets organisation.

Johan inledde med att informera om cybersäkerhetskollen, som tagits fram av MSB med syfte var att mäta nivån på verksamhetens systematiska cybersäkerhetsarbete, samt ge stöd till förbättringsarbete. Sammanlagt svarade 136 av landets kommuner på undersökningens frågor. Utfallet av undersökningen är mycket nedslående. För närvarande är det endast 6 av 136 kommuner uppfyller den rekommenderade säkerhetsnivån. Intressant nog var IT-säkerheten högre jfr med informationssäkerheten.

Under föreläsningen exemplifierade Johan konsekvenserna för Mora kommun som blev utsatt för en så kallad ”Spearphishing-attack”, eller ”nätfiske-attack”, som skedde i deras 365-miljö. Detta skedde trots att Mora sedan länge har ett väl strukturerat cybersäkerhets arbete blev de offer för en cyberattack.
Vid attacken användes en 365-applikation för data-exfiltrering, dvs införande av skadlig kod som i sin tur föder över information från ett nätverk eller system till en extern plats.

En konsekvens av attacken var att informationen som stals såldes vidare i flera led med möjligt syfte att skapa informationspåverkan, ekonomiskt bedrägeri och eller driftstörningar.

En nyhet är att den nya lagen ger kommunernas högsta ledning ansvaret för att uppfylla lagens krav. I syfte att underlätta detta kommer samtliga politiker som sitter i kommunstyrelsen ska genomgå en utbildning tillhandahållen av SKR.

Cybersäkerhet ska vara en del av kommunernas riskhantering där riskerna ska identifieras och värderas. Resurserna ska anpassas efter risknivå och de ska följa upp kontinuerligt. Johan betonade vikten av att koppla riskhanteringen till krisberedskap och kontinuitet samt att öva på krishantering i samband med ´cyberangrepp.

Riskaptit är ett centralt begrepp inom cybersäkerheten. Det innebär att utifrån en sammanvägd bild bestående av hot, externa krav, verksamhetsanalys och riskanalys definierar en riskaptit som sedan ligger till grund för det regelverk som behövs och för att ta informerade beslut om hur väl informationen ska skyddas.

Avslutningsvis betonade Johan vikten av att alltid ha säkra back-up-funktioner för vital information. Detta är extra viktigt om man skulle bli utsatt för t.ex. en s.k. ”ransomeware-attack”.
Ett tips från Johan var att gå in på SKR:s hemsida för att få hjälp och stöd avseende enkla åtgärder som ger en högre säkerhetsnivå.

Vad gör vi nu för att gemensamt leva upp till de nya kraven?
Utbildningsdagen avslutades med en gemensam diskussion om vad vi tillsammans behöver göra för att leva upp till den nya lagens krav. I syfte att undvika dubbelarbete och otydlighet beslutades att en arbetsgrupp bestående av informationssäkerhetsamordnare i V6-kommunerna, cybersäkerhetsspecialisterna på Göliska IT, inköpschef V6 inköpscentral, chefsjurist Skara kommun och förbundsdirektören Göliska IT, tar fram en plan som beskriver vem som gör vad och när för att leva upp till de nya kraven. När en tydlig ansvarsfördelning är gjord startar arbetet i respektive kommun och på Göliska IT. Arbetet kommer sedan att fortgå i modellen för objektsförvaltningen.

Arbetsgruppen startade sitt arbete den 15:e oktober. Målet är att vi på ett gemensamt strukturerat sätt kommer att leva upp till den nya lagen.

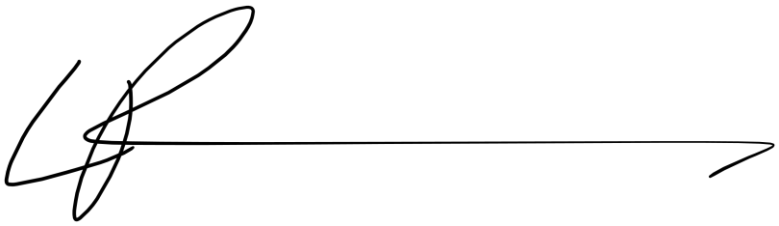
Säkerhetstips från Göliska IT
Avslutningsvis vill vi på Göliska IT ge er några enkla säkerhetstips som hjälper dig att få en mer problemfri arbetsdag:

1. Använd starka, unika lösenord. Lämna aldrig ut ditt lösenord till någon och använd olika lösenord på jobbet och privat.
2. Uppdatera din programvara och dina enheter regelbundet.
3. Var försiktig med att öppna e-post från okända avsändare eller från avsändare vars e-mailadress ser ovanlig ut. Klicka aldrig på okända länkar och filer.
4. Använd alltid skärmlås på din dator, telefon eller platta när du inte använder den.
5. Om du är osäker på om ett e-mail, en länk eller en fil är säker att öppna är du alltid välkommen att ringa till Göliska IT servicedesk 0510-77 70 00 så hjälper vi dig omgående.

Förslag till förbättringar
Vi strävar alltid efter att förbättra verksamheten och tar därför gärna emot dina förslag och idéer som hjälper oss att ge en bättre service till er alla. Du är alltid välkommen att höra av dig direkt till mig om du har några specifika frågor om verksamheten på Göliska IT eller allmänna frågor om digitalisering av kommunala verksamheter. Du är också välkommen att skicka dina förbättringsförslag till mig på nedanstående e-mailadress.

Stort tack för att du läst nyhetsbrevet. Vi kommer snart tillbaka med mer nyheter och information från Göliska IT.

Bästa hälsningar från oss alla på Göliska IT



Carl Johan Fredin

Förbundsdirektör Göliska IT

072 - 965 38 64

carl-johan.fredin@goliskait.se