Svar på interpellation från Lars Eliasson (M) – IT-säkerhet i Vilhelmina kommun

Interpellantens fråga gäller varför Vilhelmina kommun behandlar hur kommunen säkerställer att de kommunala verksamheterna fungerar vid IT-attacker. Till att börja med vill jag tacka interpellanten för den inskickade interpellationen och möjligheten att informera om det aktuella ämnet säkerhet och beredskap vid IT-attacker mot kommunen. Det är relevanta frågeställningar som berör alla kommuner i Sverige, däribland Vilhelmina kommun och dess verksamheter. Följande svar på sakfrågorna är förankrade hos kommunchef Karl-Johan Ottosson och IT-chef Jonas Örnberg:

Kommunstyrelsen, bland annat genom IT-enheten, följer sedan en god tid tillbaks händelserna i Sverige och omvärlden för att förstå mönstren och i möjligaste mån förebygga attacker, intrång och informationsförluster. Att förespå hur nästa attack kommer se ut, tillvägagångssättet, vilka som är målet för attacken och därmed också kunna förebygga angreppen är inte en enkel uppgift.

Vi har följt händelserna hos Kalix Kommun, Region Gotland, Svenska Kyrkan, COOP Värmland, Härjedalens kommun, Tieoty Evry, Vellinge kommun, Advania, Kalmar kommun, Bjuvs kommun, Sofiahemmet, Jämtlands räddningstjänst, Norrmejeriet och försökt dra lärdom av de attacker/intrång som de blivit utsatta för. Vi har för egen del också färsk i minnet när vi blev utsatta för postnordviruset 2016/2017 och konsekvenserna av detta.

1. **Hur säkerställs att kommunen inte drabbas av:**
   *** dataintrång**
   *** andra IT-relaterade manipulationer som falska mail**
   ***manipulerade telefonsamtal/sms**
   ***klonade röster**
   ***fejkade videosamtal**
   ***fullt utvecklad ”deepfake”?**

För det första tror vi på att bygga fungerande förvaltningsorganisationer där rollerna för stödsystemen är fastställda och att alla berörda vet vem som är systemägare, systemförvaltare och systemadministratör. Oavsett driftform (lokaldrift, moln, on-prem eller SAAS) behöver dessa roller finnas utpekade och alla ska veta vad som förväntas av dem.

Att helt säkerställa att kommunen inte kan drabbas av uppräknade ”attacker” är omöjligt. De onda krafterna är ofta steget före i sina intrångsmetoder. När ”främmande makt” har mållåst på en aktör med avsikt att sabotera kommer det vara mycket svårt att skydda sig. Ofta kommer insatserna då uteslutande att handla om skademinimering.

Men svaret är, genom de stödsystem som idag finns för ändamålet (nationella blixtmeddelanden genom CERT.se, brandvägg, monitorering, avvikelsebevakning), genom att kontinuerligt identifiera våra systemtekniska brister och våra konfigurationsbrister och åtgärda dessa, genom ett aktivt behörighetsarbete, genom utrangering av oskyddbar IT-utrustning och genom breda eller riktade utbildningar av personalen kring innehållet i informationssäkerhetspolicyn och informationssäkerhetsinstruktionen. Vi ser också att genom klustersamverkan, exempelvis med Regionen och AC-net, har vi tagit flera steg framåt i säkerhetsarbetet och har fått mer kunskap in i våra organisationer. Med mer resurser skulle vi

givetvis kunna få snabbare framdrift på de områden där vi genomför åtgärder men att tillskjuta mer resurser har hittills inte varit aktuellt.

2. **Vilka åtgärder har kommunen vidtagit för att säkerställa att den dagliga kommunala servicen ska kunna fungera vid en IT-attack?**

Till alla stödsystem som är klassade som känsliga finns framtaget en systemförvaltningsplan (några, men inte alla systemägare/processägare har gjort detta). Parallellt med den har systemägaren/processägaren arbetat med kontinuitetsplaner för att manuellt kunna hantera situationen som uppstår i samband med att stödsystemen skulle vara otillgängliga (några, men inte alla systemägare/processägare har gjort detta).

3. **Vilka åtgärder har kommunen vidtagit för att för att säkra att sekretessbelagda eller andra känsliga uppgifter är skyddade vid en IT-attack?**

Genom ett aktivt arbete från digitaliseringsgruppens ledamöter så hanteras idag den största delen av sådana uppgifter i det för verksamheten upphandlade stödsystemet. Dessa system är avsedda att inrymma känsliga uppgifter och skyddas oftast av flerfaktorslösning med hög tillitsnivå. Datat i dessa system backupas sedan enligt vedertagen standard och enligt verksamhetens krav. I de fall känsliga data behandlas utan verksamhetsansvarigas, digitaliseringsgruppens eller IT-enhetens vetskap (skugg-IT) finns inget skydd för den typen av uppgifter.

4. **Vilka åtgärder har kommun vidtagit för att viktig information inte ska gå förlorad om system slås ut?**

Främst genom att skärpa kraven på systemförvaltning och informationsägarskapet. Backupfrågan är central i detta sammanhang och flera av våra systemdriftande partners har kontaktats och fått redogöra för hur dess backuprutiner ser ut och i vissa fall hur de kan förbättras. Vilhelmina kommun rekryterar nu också en informationssäkerhetssamordnare som ska vara verksam och drivande kring arbetet med informationsskyddet.

Sammanfattningsvis så pågår arbetet med den här typen av beredskaps- och säkerhetsfrågor hela tiden. Ibland sägs det att ”det enda sättet att helt och hållet skydda sig mot IT-attacker är att inte använda IT över huvud taget”, andra gånger sägs att ”det är vi användare som är det största hotet när det kommer till att släppa in andra i våra system”, och det finns säkerligen mer eller mindre sanning i båda delarna. Vilhelmina kommun ligger dock väldigt bra till i det totala arbetet med IT-säkerhet, vilket jag tycker att vi ska ta med oss från den här ärendet.

Andreas Eliasson

Kommunstyrelsens ordförande

Vilhelmina 2024-05-02