CYBERSÄKERHETSLAGEN · KOMMUNER · NIS2

Cybersäkerhetslagen i kommuner

Cybersäkerhetslagen ändrar inte bara vilka krav som ställs på kommunen. Den höjer också kraven på vad kommunen måste kunna visa när arbetet ska följas upp. För IT innebär det att spridda exporter, punktinsatser och muntliga lägesbilder får allt svårare att bära. För ledningen innebär det att uppföljning måste vila på något mer robust än att arbete pågår.

- Vad lagen faktiskt kräver av kommunens uppföljning
- Varför konsultspåret inte täcker det tekniska ansvaret
- Vad IT och ledning konkret behöver kunna visa

I KORTHET

Det lagen skärper

Tyngdpunkten flyttas från enstaka aktiviteter till sådant som faktiskt går att följa upp, redovisa och koppla till riskreducering.

Det vanliga glappet

Information finns ofta, men inte i en form som håller för ledningsfrågor, revision och tillsyn.

Den praktiska konsekvensen

Kommunen behöver en återkommande bild av läget, inte punktvisa utdrag som måste tolkas om varje gång.

När lagkravet möter kommunal verklighet

Det är lätt att prata om cybersäkerhetslagen som ett regelverk på armlängds avstånd. I praktiken landar den i en enklare fråga: går det att visa ett verkligt säkerhetsläge, och går det att följa det över tid?

För många kommuner är det där friktionen uppstår. Inte för att inget görs, utan för att arbetet inte lämnar efter sig ett tydligt, återkommande och jämförbart underlag. När frågor kommer från ledning, revision eller tillsyn börjar man därför ofta samla ihop material på nytt.

Vad kommunen i praktiken behöver kunna visa

Det centrala är inte att kunna visa perfekt säkerhet. Det centrala är att kunna visa ett systematiskt arbete som går att följa.

- Hur såg läget ut vid senaste mätningen?
- Vad har förändrats sedan dess?
- Vilka åtgärder har genomförts och vilken effekt fick de?

> **Cybersäkerhetslagen skärper inte bara kraven på säkerhetsarbete.** Den skärper också behovet av något mer stabilt än punktinsatser och ad hoc-sammanställningar.

Varför konsultspåret inte räcker för den tekniska uppföljningen

För många kommunledningar är konsultspåret det naturliga första valet. Det är logiskt. En välkänd rådgivare kan hjälpa till med tolkning, ansvarsfördelning och programarbete. Men de tekniska delarna av NIS2 försvinner inte för det.

Någon måste fortfarande kunna visa hur säkerhetsläget faktiskt ser ut i kommunens miljö, vad som har förändrats sedan föregående mätning och vilka brister som fortfarande återstår. Det arbetet går inte att ersätta med en workshopserie eller ett styrdokument. Det kräver ett återkommande tekniskt underlag.

Det här behöver kommunen kunna visa

Inför tillsyn eller revision

- Vilket nuläge som gällde vid senaste mätningen
- Vad som förändrats sedan dess
- Vilka brister som fortfarande är kända
- Vilka åtgärder som har genomförts

Det IT behöver följa upp

- Patchstatus och kända sårbarheter
- EOL-system och EOL-programvara
- Endpoint-skydd och diskkryptering
- AD-hygien och miljödata från flera källor

Varför information ändå inte blir ett användbart styrunderlag

Patchstatus finns ofta någonstans. Endpoint-skydd någon annanstans. Kryptering i ett tredje system. AD-relaterade frågor i manuella utdrag. Miljödata och sårbarheter i andra verktyg eller i separata leveranser.

Det som saknas är sällan information. Det som saknas är ett format som håller. Spridd information är inte samma sak som ett underlag som går att använda i styrning, uppföljning och tillsyn.

Vad IT behöver kunna följa utan att drunkna i detaljdata

För IT är det sällan hjälpsamt att försöka följa allt samtidigt. Det viktiga är att ha ett mindre antal tekniska områden som återkommer i samma struktur och går att jämföra mellan mätningar.

- Patchstatus och kända sårbarheter
- EOL-system och EOL-programvara
- Endpoint-skydd
- Diskkryptering
- AD-hygien
- Miljödata från flera källor

Skillnaden mellan att ha uppgifter och att ha ett underlag

Data är råmaterial. Ett fastställt underlag är något organisationen kan stå för. Det innebär att man vid varje mätning faktiskt kan säga: det här var läget här och då, det här har förändrats sedan sist och det här kräver åtgärd.

Det är en annan sak än att bara kunna plocka fram uppgifter ur olika system när någon frågar.

Vad detta betyder för ledning, ansvar och uppföljning

Ledningen ska inte gå in i tekniska detaljer. Men ledningen måste kunna följa säkerhetsarbetet på ett sätt som håller över tid. När underlaget är fastställt blir det lättare att följa utvecklingen, se om åtgärder ger effekt och svara tydligare när revision eller tillsyn vill veta mer.

En rimlig väg framåt

- ✓ Samma grundstruktur vid varje mätning
- ✓ Ett tydligt nuläge
- ✓ En tydligare riskreducering över tid
- ✓ En tydligare koppling mellan åtgärd och effekt
- ✓ Ett underlag som IT kan stå för och ledningen kan använda

Var Statira kommer in

Statira är byggt för just detta läge: när arbetet redan pågår, men underlaget fortfarande är för spritt, för personberoende eller för tillfälligt för att hålla över tid.

Det gör det lättare att arbeta praktiskt i IT. Det gör det också lättare att visa var risk har reducerats när frågor kommer från ledning, revision eller tillsyn.