• Digital säkerhet

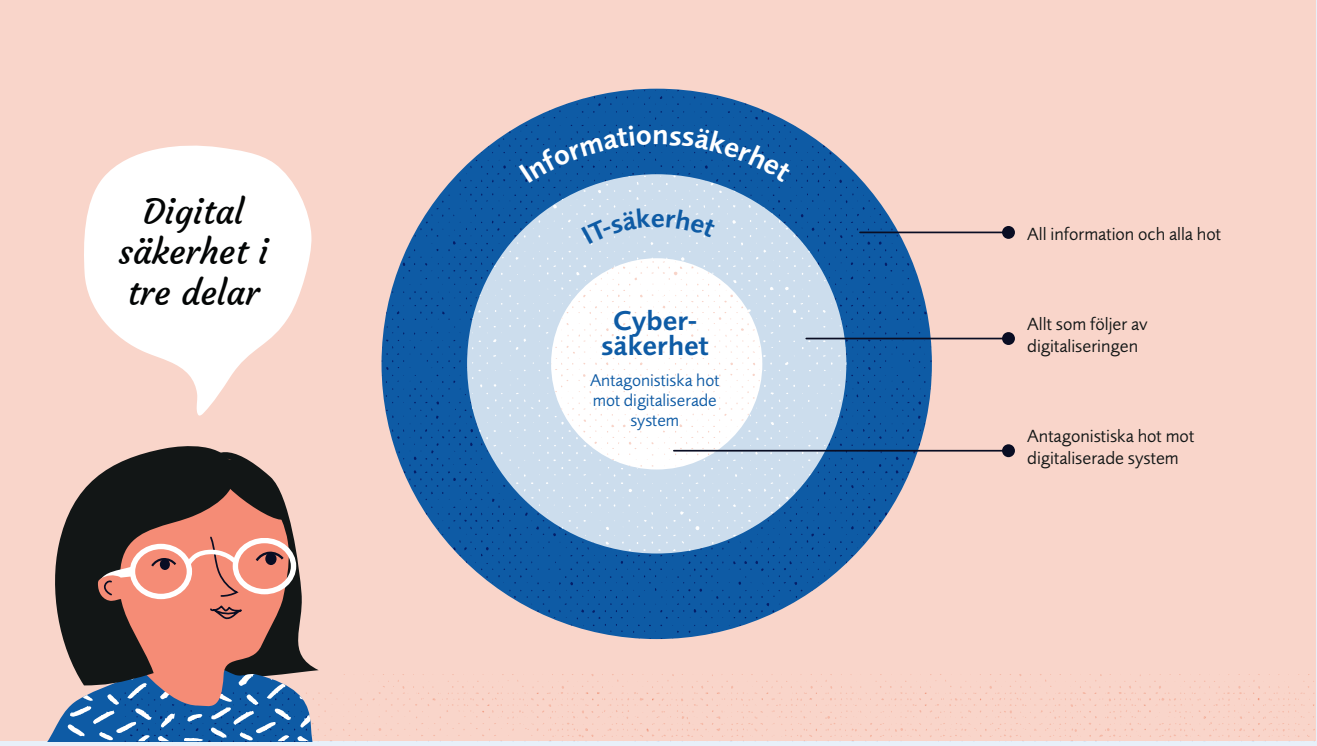
Samhället har hanterat säkerhetsfrågor under alla faser av industrialiseringen. Inriktningen på säkerhetsarbetet har präglats av rådande tekniska förutsättningar och teknikskiften, till exempel vid elektricitetens införande och det kommersiella flygets utveckling. Digitaliseringen, som ofta benämns som den fjärde industrirevolutionen, förändrar nästan alla delar i samhället och påverkar vår hantering av information. Betalsystem, affärssystem, journalsystem, logistikkedjor och energisystem med mera har sin grund i digital teknik och är i de flesta fall uppkopplade mot Internet. Det skapar enorma möjligheter men också risker som behöver hanteras eftersom samhället inte klarar längre avbrott.

En betydande drivkraft i digitaliseringen är kraven på effektivitet och förenklat arbetssätt. Detta måste vägas mot de legala och säkerhetsmässiga kraven för myndigheter och företag samt den enskilde individens integritet. Förmågan att ta hänsyn till dessa parametrar är en av digitaliseringens största utmaningar.

I takt med att allt fler människors använder sig av Internets möjligheter och att saker, platser och tjänster är uppkopplade har behovet av informationssystem och infrastrukturer som är säkra och robusta ökat. En stor mängd information hanteras av individer och inom organisationer. Information kan ses som navet, en viktig byggsten, för att bedriva en verksamhet. Det ställer krav på att informationen hanteras rätt och skyddas, den ska finnas tillgänglig när den behövs, vi måste kunna lita på att den är korrekt samt att endast de personer som är behöriga får ta del av den.

För att kunna ta vara på digitaliseringens möjligheter är det angeläget att det digitala samhället genomsyras av ett demokratiskt synsätt och att alla ska känna en grundtrygghet i den digitala samhällsutvecklingen. Alla ska våga lita på digitala tjänster och både vilja och kunna bidra till användningen av dessa. Såväl privata som offentliga aktörer behöver agera på ett ansvarsfullt sätt.

Ett sätt att översiktligt beskriva begreppet digital säkerhet är dela in det i tre delar eller nivåer[14]. Informationssäkerhet är den första nivån och omfattar skydd av all typ av information. Inte bara den digitala utan även fysisk, som talad och pappersbunden information. Nästa nivå är IT-säkerhet som omfattar skydd av digital information och digitala informationssystem från incidenter som naturkatastrofer, handhavandefel, avgrävda kablar, bränder, brister i hårdvara och applikationer etc. Den tredje nivån är cybersäkerhet och med det avses skydd av informationssystem från externa hot som avser att slå ut samhällsfunktioner eller begå brott riktade mot individer eller organisationer.



[14] *https://www.iva.se/globalassets/projekt/201902-iva-digitalisering-slutrapport-l.pdf*

Att arbeta med informationssäkerhet och IT-säkerhet är ett långsiktigt systematiskt arbete för att skydda informationstillgångar. Det innefattar framtagandet av riktlinjer, policys, handlingsplaner och klassificering av information samt att hantera tekniskt skydd som till exempel brandväggar och kryptering. Det behövs analys av sårbarhet, vilka tillgångar som är sårbara och kunskap avseende mekanismerna som kan leda till ett säkerhetshot eller en svaghet. Förutom detta krävs också att enskilda individer, såväl privat som i företag eller organisationer, har en grundläggande kompetens och förståelse för digital säkerhet, till exempel om lösenordshantering och försök till bedrägerier via olika digitala kanaler för att minska sårbarheten.

Vår omvärld förändras kontinuerligt och säkerhetsläget har försämrats med en ökad risk för cyberattacker och sabotage. Säkerhetsarbete handlar även om att bygga upp datorsystem som klarar såväl externa attacker som systemfel eller utrustning som förstörs. För offentliga och civilsamhällesaktörer är det en fråga om att kunna skydda individernas trygghet och demokratin, medan det för företagen också handlar om att skydda sin affärsverksamhet, teknologi, forskning och utveckling. Detta kan handla om olika typer av lösningar till exempel genom molnlösningar som skyddar informationen om den egna servern havererar.

Samtidigt finns utmaningar i att lagra information på externa servrar som kan ligga i andra länder. Större företag och organisationer har ofta resurser för att utveckla resiliens, men för mindre aktörer och i synnerhet små företag och föreningar kan detta arbete innebära alltför stora kostnader. För att skapa förutsättningar för en digital trygghet och säkerhet i samhället behöver vi i Västerbotten utveckla och stärka vår samverkan såväl lokalt som regionalt samt koppla det till de nationella strukturer som exempelvis myndigheten för samhällsskydd- och beredskap (MSB) ansvarar för.

Nyckelåtgärder

- Kompetensutvecklingsinsatser för ökad kunskap och förmåga till digital säkerhet hos företag, offentliga aktörer och civilsamhälle.
- Utveckla eller vidareutveckla lokala eller regionala modeller som stöder företag, offentliga aktörer och civilsamhällesaktörer i analys och anpassning av säkerhetsinsatser, lagar och direktiv.
- Utveckla eller vidareutveckla regionala eller lokala samverkansmodeller som stärker samhällets digitala säkerhet och resiliens.