tillväxt verket

Informations-säkerhet

Små och medelstora företags förmåga att digitalisera och växa i en värld där informations- och cybersäkerhet blir allt viktigare.

Rapport 0339

Vi stärker Sverige genom att stärka företagens konkurrenskraft

Tillväxtverket ska skapa så bra förutsättningar som möjligt för företag i hela landet att vara konkurrenskraftiga. Det innebär att vi öppnar dörrar och river barriärer – för ett Sverige där fler företag vill, kan och vågar.

Kunskap, nätverk och finansiering är våra viktigaste verktyg. Tillväxtverkets insatser skapar direkta resultat hos de företag och aktörer som vi samverkar med, men även förutsättningar för företag och regioner att möta framtidens utmaningar. Vårt största enskilda uppdrag är att bidra till att EU-medel investeras i projekt för regional konkurrenskraft och sysselsättning.

Tillväxtverkets publikationer kan laddas ner på tillvaxtverket.se. Vill du beställa en tryckt publikation eller söker du en publikation som publicerades innan 2015 hänvisar vi till vår webbshop publikationer.tillvaxtverket.se.

Stockholm, september 2020
ISBN digital: 978-91-88961-68-6
Rapportnummer: 0339

Har du frågor om denna publikation, kontakta:
Karin Östberg
Telefon, växel 08-681 91 00

Förord

Tillväxtverket arbetar för att stärka företagens konkurrenskraft. Genom kunskap, nätverk och finansiering skapar vi bättre förutsättningar för befintliga och framtida företag och attraktiva regionala miljöer där företag utvecklas.

Digitaliseringen innebär att allt fler små och medelstora bolag kan växa både nationellt och internationellt. Små och medelstora företag kan agera som bara de stora kunde tidigare, men med nya och allt fler digitala lösningar ökar också sårbarheten. I detta sammanhang blir säkerhetsfrågorna allt viktigare. Digitalisering och informationssäkerhet är frågor som i högsta grad går hand i hand. Det är frågor som stöttar ett hållbart och konkurrenskraftigt företagande. Ett sätt att stärka affärsverksamheten är att utveckla företagens förmågor inom informations- och cybersäkerhet.

Denna rapport är framtagen i form av en kartläggning och som ett kunskapsunderlag inom ramen för Tillväxtverkets regeringsuppdrag för att höja kompetensen kring digitalisering i små företags ledningar och styrelser. Syftet är öka kunskapen om behoven av informationssäkerhet hos mindre företag, särskilt hos tillväxtföretag med mer avancerade affärsmodeller, företag som utvecklar digitala produkter och företag som delar information i ekosystem av olika organisationer, samarbetspartner, leverantörer och kundföretag.

Magnus Burvall, Syntesia AB har på uppdrag av och i nära dialog med Tillväxtverket skrivit denna rapport. Tillväxtverket har bearbetat rapporten och också kortat denna något. Författaren står för sakinnehåll, slutsatser och rekommendationer.

Vi hoppas att denna rapport kan utgöra ett kunskapsstöd inför framtida satsningar för att stärka mindre företags tillväxt genom informationssäkerhetsarbete.

September 2020

Tim Brooks
Avdelningschef
Tillväxtverket

Karin Östberg
Projektledare
Tillväxtverket

Innehåll

Sammanfattning

Digitaliseringen möjliggör för mindre företag att växa snabbare och att skala upp verksamheten internationellt. Sverige rankas ständigt mycket högt i internationella mätningar när det gäller innovation, men inom säkerhet hamnade Sverige först på plats 20 i Europa enligt Global Cybersecurity Index (GCI), 2018. I takt med att företagens affärer och tillgångar digitaliseras blir säkerhet en affärskritisk fråga. Det är viktigt att digitalisering och informationssäkerhet går i takt. Attackerna har dessutom ökat dramatiskt de senaste åren i spåren av en ökad digital utveckling.

Informationssäkerhet handlar om att skapa rätt förutsättningar för verksamhet och affär i en värld där digitaliseringen sker in allt snabbare takt. I många företag ligger så mycket som 80 procent av värdet i data och information.

Den digitala ekonomin är en ”beroendeekonomi” där kraven är att hålla samma säkerhetsnivå genom olika typer av s.k. ekosystem och leverantörskedjor. Lagstiftning, regelverk och de stora företagen sätter spelreglerna. Det gäller för de små att hänga med.

Informationssäkerhet handlar både om affärsmöjligheter och riskhantering. Tre av fyra företag råkar ut för större eller mindre cyberincidenter enligt *World Economic Forum Global Risk Report 2019.* En attack riskerar inte bara att förstöra data och nätverk utan också kundrelationer och varumärken.

Stora företag, börsbolag och banker satsar avsevärda medel och resurser på säkerhetsarbete. Trots detta är säkerhetsfrågorna en ständig oro för styrelse och ledning hos våra storbolag. För små och medelstora företag är utmaningarna annorlunda men minst lika stora. Här handlar det i ännu högre utsträckning om prioriteringar eftersom de har begränsade resurser och kompetens. Företagens behov och efterfrågan av experter, av konsultstöd och rådgivning inom informationssäkerhet matchar inte alltid marknadens erbjudanden. Det ställer krav på ägare, styrelse och ledning i de mindre företagen att ha tillräckliga kunskaper och kompetens för att kunna arbeta systematiskt, strategiskt och att kunna göra rätt prioriteringar.

Genom att arbeta strategiskt med säkerhet kan ett företag skapa konkurrensfördelar. Men säkerhet kostar pengar och det gäller att ha en relevant digital strategi och tillgång till rätt kompetens. Företaget behöver identifiera vad som är skyddsvärt och vilken typ av information och data som är viktigast att skydda i företaget.

Alla små och medelstora företag behöver ett basskydd. Men teknik i sig är aldrig en tillräcklig säkerhetslösning. Faktum är att den största säkerhetsrisken i ett företag är den omedvetna medarbetaren. Det behövs därför att styrelse och ledning går i bräschen för att skapa säkerhetskulturen i företaget.

Det är stor skillnad på digital mognad och krav på säkerhet i de små och medelstora företagen - baserat på företagens affärsmodell, typ av produkter och roll på marknaden. De små och medelstora företagen är allt annat än en homogen grupp.

Behovet att höja kunskap om informations- och cybersäkerhet hos styrelse och ledning är fortsatt stort. Bristande kunskaper riskerar att bli en barriär för tillväxten i svenska små och medelstora företag. Det finns även brister i marknadsutbudet är det gäller säkerhetskompetens och tjänster anpassade för de små och medelstora företags behov. I rapporten lyfts ett antal områden fram där utmaningarna och de digitala affärsriskerna är som störst för bolag med tillväxtambitioner.

1 Inledning

Rapporten är tänkt att vara ett kunskapsunderlag och delvis också ett stöd i genomförandet av Tillväxtverkets regeringsuppdrag *"Uppdrag att utveckla och genomföra ett program för att höja kompetensen om digitalisering i små företags ledningar och styrelser".*

Informationssäkerhet tas oftast upp i perspektiv av hot, intrång och annan IT-relaterad brottslighet. Taktiken handlar därför om att skydda sig eller att "släcka bränder". Men för de företag som arbetar strategiskt med informationssäkerhet finns även stora affärsmässiga möjligheter. Detta är huvudperspektivet för denna rapport.

Informationssäkerhet är, precis som digitalisering, ett komplext område med många olika utmaningar för företag och organisationer. Det finns ett behov för alla människor i samhället av att ha en grundläggande kompetens inom informationssäkerhet. För företag varierar behoven - allt från att ha ett basskydd för sin verksamhet till mer avancerade skydd och rutiner i företag och företag som delar data i ett ekosystem av olika aktörer.

1.1 Syfte

Syftet med denna studie är att kartlägga och försöka förstå behoven hos målgruppen små och medelstora tillväxtföretag, dvs i detta sammanhang företag med mer avancerade affärsmodeller, företag som utvecklar digitala produkter och företag som delar information i ekosystem av olika organisationer och företag. Den ska även identifiera och föreslå områden för framtida insatser för att stötta små- och medelstoras arbete med informationssäkerhet.

1.2 Metod för kartläggningen

Kartläggningen är genomförd via desktop research, intervjuer med företagsfrämjare samt genom intervjuer med experter inom informations- och cybersäkerhet.

Med företagsfrämjare innefattas företags-, affärs- eller innovationsfrämjare – i detta fall företagsrådgivare, inkubatorer, teknikparker och innovationskluster:

- IGNITE Sweden (www.ignite sweden.org)
- THINGS (www.thingsstockholm.com)
- Automation Region (www.automationregion.com)
- IoT Sweden (www.iotsweden.se)
- Linköping Science Park (www. linkopingsciencepark.se)
- RISE (www.ri.se)

Intervjuer är genomförda med ett antal experter inom informationssäkerhet, cybersäkerhet och dataskydd för att fördjupa kunskap, särskilt med fokus på målgruppen små och medelstora tillväxtföretag samt startups.

2 Säkerhetsfrågor - en megatrend

Samhället, myndigheter och företag har tacklat säkerhetsfrågor under alla faser av industrialiseringen. Det gäller allt från hantering av elektricitet, hållfasthet hos byggnader och annan infrastruktur till det avancerade säkerhetstänkandet inom flyget. Inriktningen på säkerhetsarbetet har bestämts av de tekniska förutsättningarna.

Den digitala utvecklingen förändrar nästan alla delar av samhället och påverkar företags hantering av information. Betalsystem, affärssystem, logistikkedjor, energisystem, infrastruktur, styrning av städer med mera har sin grund i digital teknik. Samhället klarar inte längre avbrott. Till stöd för företag finns mängder av IT-utrustning, IT-program och digitala tjänster för att hantera, lagra och överföra information. Detta skapar möjligheter att arbeta effektivt och att utveckla företaget, men det skapar också risker.

Omfattningen av insatserna har påverkats av samhällets syn på risker och riskhantering, ofta formulerade i politiska processer. Digitaliseringen, den fjärde industriella revolutionen, innebär att nästan alla verksamheter är beroende av IT-system och därmed IT-säkerhet.

Trenden mot ökad digitalisering av företag och samhälle skapar ett allt större beroende av digitaliserad information. Utbytet av stora datamängder internt och externt på global nivå gör organisationer till ett attraktivt byte för cyberbrottslighet.

Företag som baserar sin verksamhet på olika teknologier, exempelvis Internet of Things, IoT, förlitar sig i stor utsträckning på global digitalisering för sin tillväxt. I takt med att systemen blir mer komplicerade, sammankopplade och hanterar mer information, blir exponeringen för attackytan mycket bredare, samtidigt som luckorna i säkerhetssystemen exponeras. Tittar vi framåt så är de primära plattformarna för ökade cyberbrottsaktiviteter big data, molntjänster, sociala medier och mobila tjänster.

Tredjepartsdatalagring och molnbaserade tjänster har öppnat upp vägar för online-attacker som tidigare inte fanns. Dessutom kan IoT-produkter som är aktiverade med IP-sensorer, och som inte testats tillräckligt, göra användardata sårbar för attacker.

Säkerhetsarbetet, under den fas av digitalisering som vi är inne i just nu, påverkas av ett antal megatrender[1]:

- *Det samlade värdet på digitala system ökar.* Värdet ska ses dels som de direkta intäkter och besparingar som uppkommer genom användningen av systemen, dels som kostnader för att använda alternativa lösningar. Uppskattningar visar att uppemot 70–85 procent av en verksamhets tillgångar är digitala.

- *De digitala systemen grundas på allt färre tjänster som tillhandahålls av ett mindre antal producenter*. Swish och BankID är två exempel. Om dessa slutar att fungera blir konsekvenserna omedelbara och omfattande. Om ett viktigt betalningsmedel (Swish) skulle stängas ned går inte att sköta bankaffärer och myndighetskontakter (BankID).

[1] Digitalisering för ökad konkurrenskraft, IVA, 2019

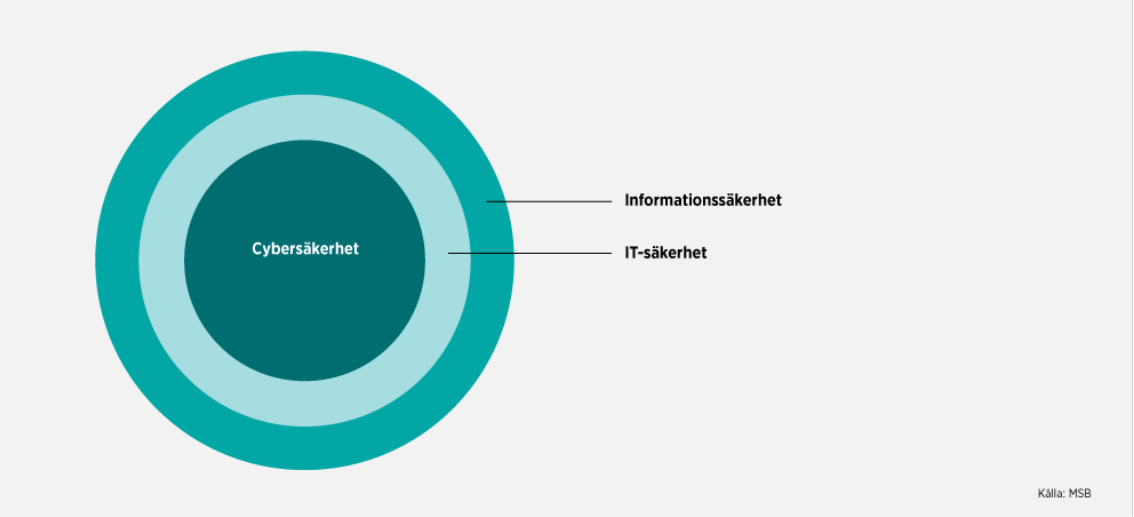
- *Vårt samhälle bygger på en ökad användning av internet och internetteknik*. Detta gäller för såväl grundläggande samhällsfunktioner som i individernas vardag. Därmed ökar exponeringen för attacker från enskilda hackare och organisationer.

- *Allt större brist på kompetens och kunskap för att bedöma och hantera risker.* Antalet specialister inom det komplicerade säkerhetsområdet är redan idag få, och minskar jämfört med behovet. Det finns också brister i kunskaper och insikter hos politiker och andra beslutsfattare om riskernas karaktär, omfattning och hantering *(Källa: ESV 2018).*

- *Den tekniska utvecklingen* med exempelvis mobilitet, IoT (Internet of Things eller sakernas internet på svenska), kvantdatorer, big data, virtualisering, robotisering och automatisering innebär nya hot och risker. Men samtidigt ger utvecklingen utrymme för innovativa lösningar på säkerhetsområdet.

2.1 Vad är informationssäkerhet, cybersäkerhet och IT-säkerhet?

Vi kan tala om tre nivåer av säkerhet:



- **Informationssäkerhet** – omfattar skydd av all information, inte bara den digitala säkerheten utan också den fysiska exempelvis den talade och pappersbundna.

- **IT-säkerhet** – allt som omfattar skydd av digital information / IT-baserade informationssystem, exempelvis genom naturkatastrofer, handhavandefel, felbedömningar, avgrävda kablar, bränder, brister i hårdvara och applikationer etc.

- **Cybersäkerhet** – den delmängd av informationssäkerhet som omfattar skydd av informationssystem mot antagonistiska hot* om att slå ut samhällskritisk verksamhet, eller att genomföra brott riktade mot individer, exempelvis identitetsstölder, kontokorts- och investeringsbedrägerier

* antagonistiska hot kommer från organisationer med både avsikten och förmågan att realisera angrepp direkt mot säkerhetskänslig och samhällsviktig verksamhet. Detta kan i förlängningen också kan destabilisera en nation

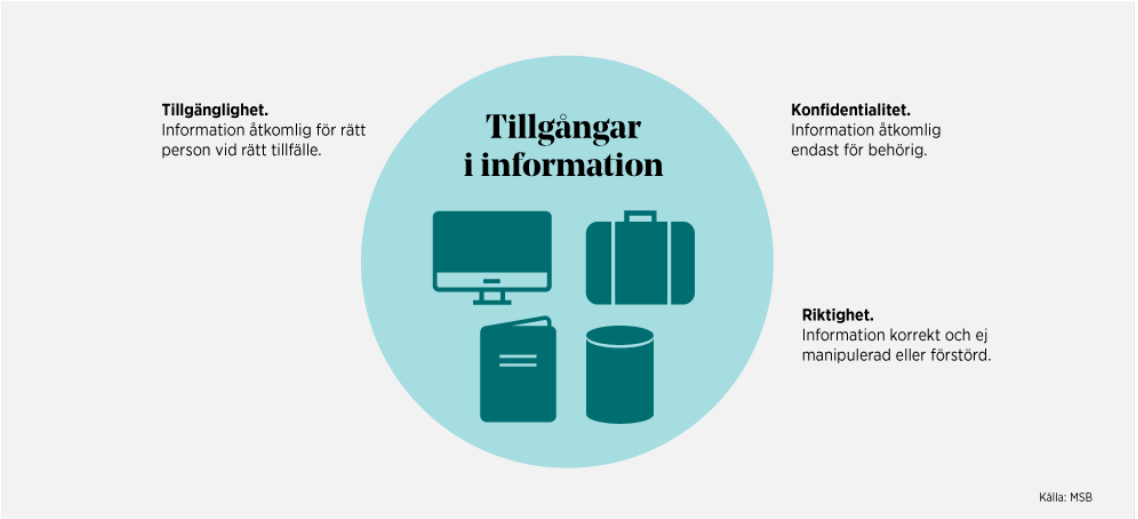
Informationssäkerhet handlar om att skapa rätt förutsättningar för affärer, för affärs- och verksamhetsutveckling i en värld där digitaliseringen sker i allt snabbare takt. Uppskattningar visar att 70–85 procent av en företags tillgångar är digitala *(Källa: Eurobanks 2017).*

Informationstillgångar finns i många former, till exempel människor med sin kunskap och kompetens, i lokaler, digital information och information på papper. Genom ett systematiskt arbete med informationssäkerhet som bygger på etablerade standarder kan organisationer öka kvaliteten i och förtroendet för sin verksamhet.

Informationssäkerhet omfattar både administrativa rutiner med policy och riktlinjer, samt *tekniskt skydd* med bland annat brandväggar och kryptering. Det handlar om att ta ett helhetsgrepp och skapa en fungerande långsiktig process för att ge organisationens kritiska information det skydd utifrån krav från verksamheten, lagar, kunder och andra intressenter.

Informationssäkerhet handlar både om digital och fysisk säkerhet

Informationssäkerhet innebär i grunden att hantera information säkert genom att begränsa behörighet till information (*konfidentialitet*), se till att information är korrekt och inte ändrad eller förstörd (*riktighet*) och att information finns tillgänglig vid behov (*tillgänglighet*). Informationssäkerhet handlar om all information i ett företag oavsett hantering i IT-system, på papper eller i människors huvuden.



Balansera arbetet med informationssäkerhet

Informationssäkerhet innebär ett riskbaserat arbetssätt vid hantering av information samt införandet av de skyddsåtgärder och rutiner som behövs. Skyddsåtgärder ska vidare balanseras mellan skyddsvärdet, hot och kostnad, en så kallad riskoptimering.

Cybersäkerhet – skydd från cyberhot

Ordet cybersäkerhet används ofta i svenskt språkbruk, men har ingen entydig definition. Ofta avses ett företags arbete med IT-säkerhet. Ett försök till definition av ordets innebörd skulle kunna vara skydd och försvar av datorer, servrar, mobila enheter, elektroniska system, nätverk och data mot skadliga angrepp. Den kallas även *informationstekniksäkerhet* eller *elektronisk informationssäkerhet*. Termen är bred och omfattar allt från datorsäkerhet till katastrofåterställning och slutanvändarutbildning. Ofta delas hoten in i cyberbrott, cyberspionage och cyberterrorism.

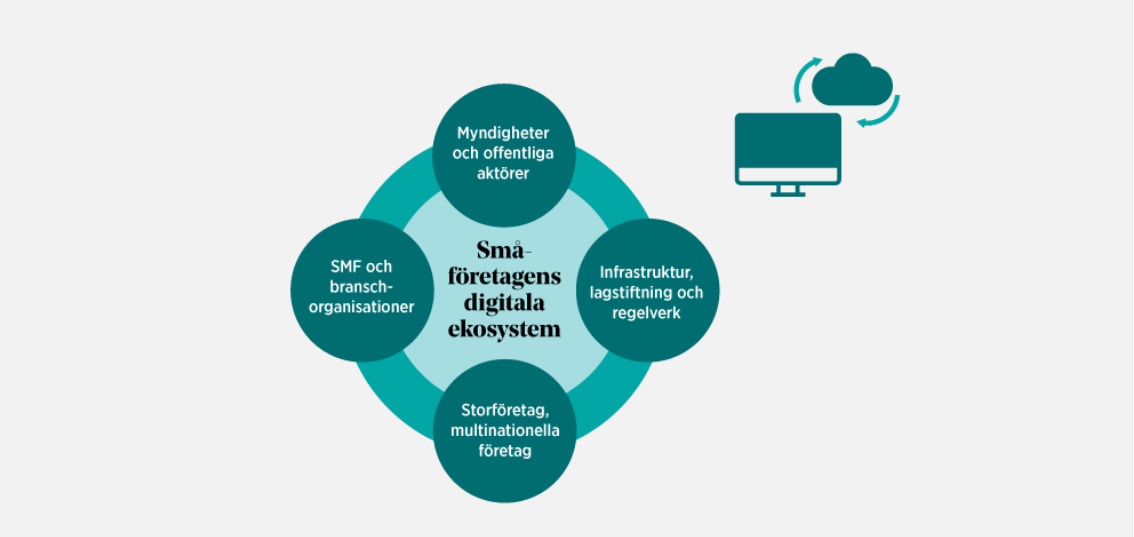
3 Digitalisering, informationssäkerhet och personlig integritet måste gå i takt

En genomgripande samhällsförändring

En studie från McKinsey Global Research bedömer att värdet som digitaliseringen årligen kan ge Sverige från år 2025 kan beräknas till mer än 850 miljarder kronor [2]. Det ekonomiska värdet uppkommer när några viktiga tekniktrender slår igenom i samhället och ekonomin. Det mest framträdande är automatisering och avancerad dataanalys (till exempel robotteknik och autonoma fordon) samt uppkoppling, molntjänster och kommunikation (till exempel mobilt internet och Internet of Things, IoT).

En viktig faktor som driver på utvecklingen är samarbetet i form av framväxande ekosystem: inom och mellan branscher, näringsliv, offentlig sektor och akademi samt mellan etablerade aktörer och nystartade företag.

Småföretagens digitala ekosystem



Figur Tillväxtverket: Småföretagen deltagande i, samarbete med och beroendeställning till olika digitala ekosystem och digitala delningsplattformar

[2] Möjligheter för Sverige i digitaliseringens fotspår, McKinsey 2017

”Digitaliseringen innebär en genomgripande samhällsförändring. Kärnan utgörs av den snabba tekniska utvecklingen, där möjligheterna att hantera stora datamängder är central. Förändringen går snabbt. Vi använder internet för en rad vitala samhällsfunktioner utan att ha försäkrat oss om att kapacitet och driftsäkerhet är tillräckliga. En rad nya frågeställningar aktualiseras, inte minst kring cybersäkerhet”.

IVA, Digitalisering för ökad konkurrenskraft.

3.1 Informationssäkerhet är en förutsättning för fortsatt digitalisering

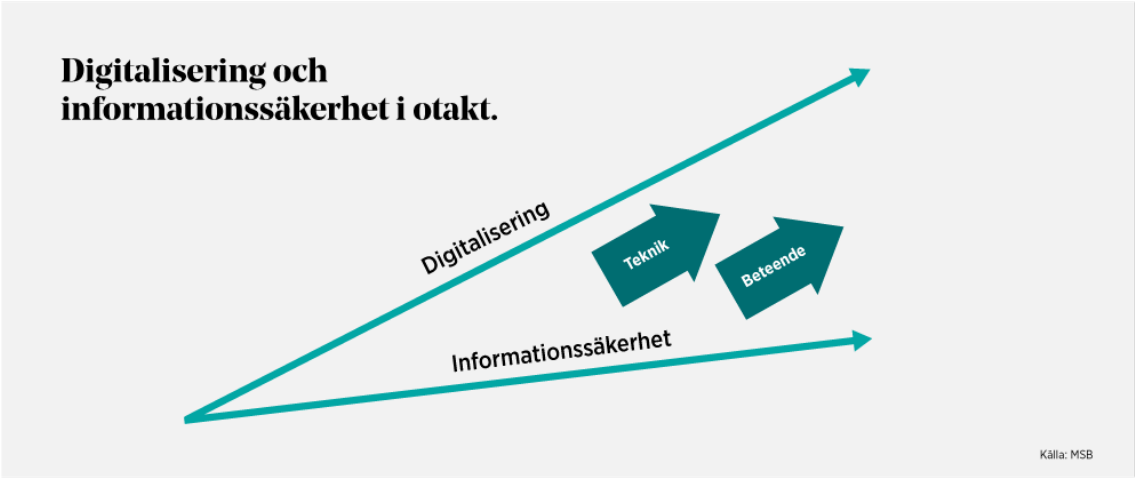
I takt med att företagens affärer och tillgångar digitaliseras blir säkerhet en allt viktigare fråga. Med digitaliseringen kommer nya utmaningar och Sverige ligger inte lika långt fram inom cybersäkerhet som inom innovation.

Digitaliseringen har påverkat oss sedan 1960-talet och vi befinner oss i en tid med accelererande förändringstakt. Från pc:ns genombrott på 80-talet, via internet på 1990-talet till att vi nu ser en utveckling mot att fler maskiner och apparater blir uppkopplade och ökade inslag av artificiell intelligens, AI.

Sverige har en lång tradition av internationellt verksamma företag. Det har varit en naturlig konsekvens av att vi har en liten hemmamarknad. Digitaliseringen har gjort att även små och medelstora företag snabbare än tidigare kan skala upp och växa internationellt. Detta påverkar också arbetet med informations- och cybersäkerhet.

Sverige – inte högt rankad

Sverige rankas ständigt högt i internationella mätningar när det gäller innovation. Exempelvis så rankades Sverige som nummer ett i European Innovation Scoreboard 2019. I Global Cybersecurity Index (GCI) 2018 hamnade Sverige först på plats 20 i Europa och nummer 32 globalt.



Företagens värde finns i information, data, produkter och varumärken

En stor del av företagens värde finns i form av digitala produkter, kunskap, data, algoritmer och inte minst varumärken. Företag är uppkopplade och starkt beroende av IT-system. Information och data utgör därför en viktig tillgång i företagen. Företag befinner dessutom i digitalt ett system av kunder, leverantörer och samarbetspartner.

4 Säkerhetsfrågor allt mer komplexa

4.1 En explosion och mångfald av enheter kopplade till internet

Utvecklingen går mot allt mera komplexa nätverk och ett ökat beroende av nätverksbaserade tjänster inom alla delar av samhället. Detta ökar kraven på säkerhet och kvalitet.

Antalet enheter som är anslutna till internet, inräknat maskiner, sensorer och kameror som utgör Internet of Things (IoT), fortsätter att växa i en stadig takt. En ny prognos från *International Data Corporation (IDC)* uppskattar att det kommer att finnas 41,6 miljarder anslutna IoT-enheter, eller "saker", vilket genererar 79,4 zettabyte (ZB) data år 2025. Det handlar om en mångfacetterad palett av enheter som vi kommer att ha i hemmet, på arbetet och i samhället. Exempel på sådana enheter är smarta hem-enheter, ”wearables”, spelkonsoler, kameror, uppkopplade fordon, smarta TV-apparater, smarta högtalare och displayer, annan internet-media, smarta mobiltelefoner, datorer och så klart också alla företagsorienterade IoT-enheter.

4.2 Den digitala ekonomin – en beroendeekonomi

Den digitala utvecklingen påverkar startups och scaleups samt små och medelstora företag med mer komplexa affärsmodeller då de ingår i ekosystem av organisationer, företag och myndigheter där data delas. Kraven ökar på företagen att hålla samma säkerhetsnivå i ekosystem och värdekedjor. De mindre företagen måste också hänga med. Det gäller inte minst i styrelse och ledning där de i tid måste tänka och agera i säkerhetsfrågor. Hur de små företagen klarar av att integrera säkerhetsfrågorna i sina affärsstrategier kan få konsekvenser då företagen söker extern finansiering, särskilt riskkapital, och vid affärer med storbolag.

Det handlar om att kunna göra rätt avvägningar av vad som är skyddsvärt och hur man ska investera för att hantera kund-, samarbets-, leverantörs-/underleverantörs- och tredjepartsrisker.

Tredjepartsrisker

Tredjepartsrisker innebär att företag exponeras mot andra företag, kanske framför allt leverantörer. Riskerna kan växa med en ökande internationalisering och globalisering. Cybersäkerhet är en viktig aspekt av vid leverantörssamarbeten och outsourcing av verksamhet. Enligt *PwCs undersökning Cyberhoten mot Sverige 2019* så ökar de s.k. tredjepartsriskerna markant. Det är viktigt att kartlägga vilken information som finns hos tredje part, att sätta tydliga krav och att ha en plan för om leverantörerna brister i säkerhetsarbetet. Det är viktigt att systematiskt följa upp tredjepartsrisker och att integrera dessa frågor i övrig internt riskhanteringsarbete.

Vikten av att förstå och respektera personlig integritet

Personlig integritet är en grundläggande rättighet. Integritet gör att vi kan skydda oss mot oberättigade störningar i våra liv. Sekretess hjälper oss att begränsa vilka som har tillgång till våra organ, platser och saker, vår kommunikation och information. Lagstiftningen som skyddar vår integritet ger oss möjlighet att hävda våra rättigheter. Teknik har alltid sammanflätats med denna rättighet. Möjligheten att skydda integriteten är större idag än någonsin tidigare, samtidigt som övervakningen och identifieringen av oss som individer genom analys av datatrafik och dataströmmar är större än någonsin. Det är nu möjligt för

företag och regeringar att övervaka varje konversation och varje kommersiell transaktion vi gör och varje plats vi besöker. Felaktigt använt kan detta leda till negativa effekter för individer, grupper, företag och t o m för samhällen och stater.

Över 130 länder har konstitutionella rättigheter om skydd av privatlivet. En viktig del av rätten till integritet är skyddet av personuppgifter. Även om rätten till dataskydd kan härledas från den allmänna rätten till integritet, föreskriver vissa internationella och nationella regelverk också en mer specifik rätt till skydd av personuppgifter.

Klagomål mot personsökningssajter

Datainspektionen publicerade i början av 2020 en rapport av som beskriver och analyserar de enskilt vanligaste klagomålen som kommer in till myndigheten. I topp hamnar sajter som masspublicerar personuppgifter som hämtas och sammanställs från svenska myndigheter. Somliga av sajterna publicerar information om personer som förekommer i brottsmål eller har fått strafföreläggande.

Närmare var femte klagomål som Datainspektionen tagit emot sedan den nya och förstärkta dataskyddsförordningen, GDPR, trädde i kraft i maj 2018, rör personsöktjänster. Totalt rör det sig om över 750 klagomål. Av klagomålen till Datainspektionen framgår att medborgare upplever personsöktjänster på internet som ett stort integritetsintrång. Även om uppgifterna är offentliga hos svenska myndigheter blir de betydligt mer lättillgängliga på personsöktjänsterna. Många som klagar är oroliga för att informationen ska utnyttjas av kriminella för att exempelvis utföra id-kapningar, bedrägerier eller inbrott.

Företagen bakom personsöktjänsterna publicerar uppgifterna med stöd av ett så kallat frivilligt utgivningsbevis, vilket gör att de till stora delar är undantagna från reglerna i dataskyddsförordningen.

Källa: Datainspektionen

För tillväxtföretag inom hårdvara, mjukvara eller som har digitala affärsmodeller måste säkerhetsfrågorna ständigt finnas på agendan hos styrelse och högsta ledning. Exemplet nedan från Zoom illustrerar hur snabbt ett digitalt bolag kan växa internationellt och vilka konsekvenser bristande säkerhetsfrågor kan få.

Zoom – en videoprogramvara som gått från 10 miljoner användare per dag till 200 miljoner på några månader.

I spåren av covid19-pandemin exploderade efterfrågan av videokonferensprogram. Ett av dessa kommunikationsverktyg, Zoom, hamnade i rampljuset. Den kraftiga efterfrågan, bland både privatpersoner och företag, bidrog till att avslöja ett antal sekretess- och säkerhetsutmaningar hos plattformen. Företaget hamnade i en storm av kritik från olika håll, däribland företrädare för sekretessfrågor, säkerhetsexperter, flera amerikanska advokater, en amerikansk lagstiftare och FBI.

Nedan de viktigaste frågorna som Zoom tvingandes hantera:

- Zooms sekretesspolicy nämnde inte att iOS-versionen av dess app skickade analysdata till Facebook, även för användare som inte har ett Facebookkonto. Detta problem är nu åtgärdat

- Trots påståenden om motsatsen stöttade inte appen video- och ljudmötenas slutkryptering, enligt forskning från The Intercept.
- Det visade sig att appen innehöll flera säkerhetsproblem som nu alla är fixade, b la att en sk UNC-injektionsfil kunde avslöja användares Windowsuppgifter.
- FBI släppte en varning av ett fenomen kallat ”Zoom-bombning” efter flera rapporter om nättroll och skojare som invaderade möten för att visa störande bilder.

Källa: Aktuell Säkerhet, april 2020.

Enligt Computer Sweden ledde säkerhetsproblemen även till en stämningsansökan av företaget Zoom av en grupp investerare då oron kring tjänstens säkerhet har påverkat aktiepriset[3].

[3] Computer Sweden, 2020-04-09.

5 Informationssäkerhetsarbete kan ge konkurrensfördelar

5.1 Förebyggande informationssäkerhetsarbete

Informations- och cybersäkerhet är fortfarande något som ibland hanteras av någon enskild funktion i företaget, oftast en IT-avdelning eller en enskild IT-ansvarig person. För bolag med avancerade affärsmodeller är dessa frågor högsta grad något som berör alla delar av ett företags verksamhet och organisation.

Den digitala ekonomin berör de flesta företag och ställer krav på att hålla samma digitala nivå och säkerhetsnivå i ekosystem och leverantörskedjor. Säkerhet är därför i högsta grad en fråga som behöver hanteras på styrelse- och ledningsnivå. Det är en stor utmaning för alla företag, även för stora internationella företag som har resurser att ta in de bästa rådgivarna och experterna i världen. Det råder global kompetensbrist inom kunskapsdomänen cybersäkerhet. Under år 2017 fanns behov runt om i världen av att anställa ytterligare 1 miljon personer inom cybersäkerhet. Positioner som inte kunde tillsättas för att det saknas utbildade personer[4].

”I en värld där data och information är i digitalt format, blir förmågan att hantera, styra och säkra data allt viktigare. De företag som hanterar sina uppgifter på bästa möjliga sätt skiljer ut sig från resten av företagen i sin kategori”.

PWC Cyber Security, 2020

5.2 Inventering av skyddsvärd information och data

Genom att integrera digitala affärsrisker och digital säkerhet kan ett företag skapa konkurrensfördelar. Säkerhet kostar pengar och det gäller att prioritera rätt utifrån storlek på företaget och dess exponering: Vad är skyddsvärt? Vilken typ av information och data är viktigast att skydda? Planerar företaget att ta in extern finansiering, särskilt riskkapital? Planerar företaget att göra affärer med stora internationella företag? Då kommer det sannolikt upp krav på att säkerhetslösningar följer branschstandarder och regelverk.

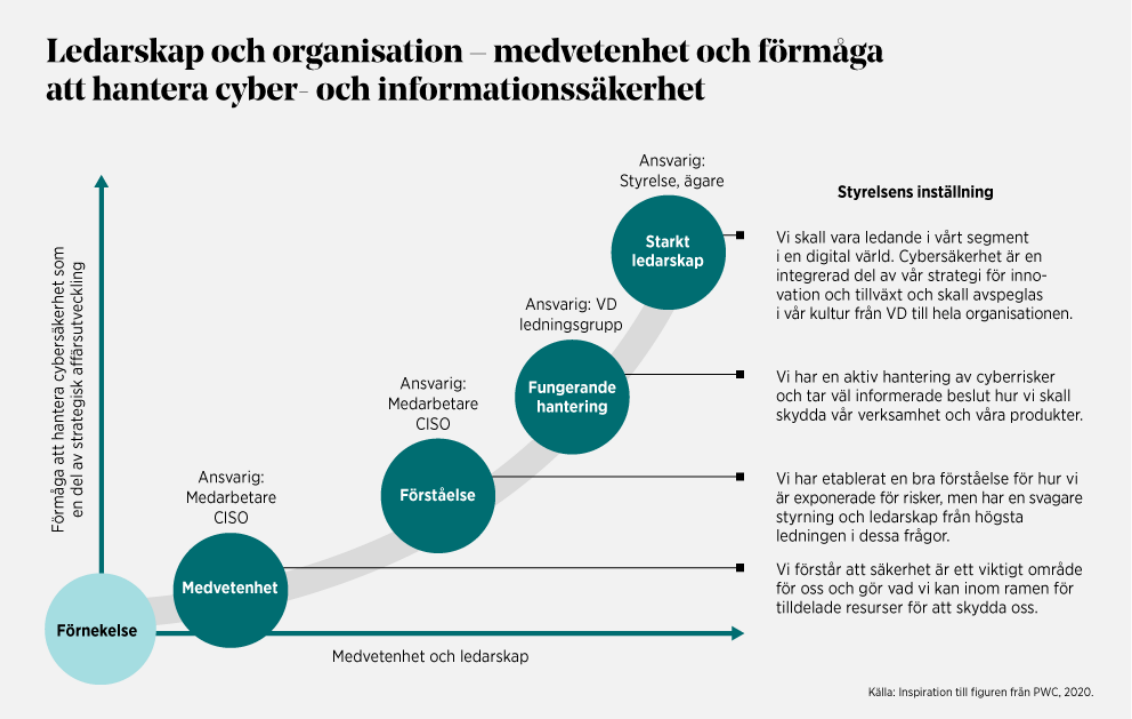
[4] Källa: Cybersecurity Ventures, Cybersecurity Jobs Report, June 2017.

Planering och fördelning av roller i företaget

Funktion	Exempel på frågeställningar
Styrelse	Hur vet vi att företaget har system för att kunna skala upp och samtidigt vara bland de bästa inom säkerhet? Har vi rätt information för att kunna bedöma företagets exponering för cyberrisker? Har vi beredskap och en testad plan för cyberincidenter?
VD	Har vi koll på den snabba utvecklingen av cyberrisker och vad den betyder för vårt företag? Har vi en tydlig strategi för cybersäkerhet som går att kommunicera i organisationen?
Produktansvarig	Respekterar vår organisation personlig integritet när vi använder data? Har vi en design på våra produkter som gör att vi klarar av att följa GDPR?
Marknad och försäljning	Utnyttjar våra system framsteg inom cyber- och integritetsriskhantering för att öka ekonomisk prestanda? Hur bibehåller vi förtroende och tillit hos kunder och konsumenter?
Säkerhet och integritet	Hur mäter och demonstrerar vi vår förmåga att hantera cybersäkerhet och integritetsfrågor för att bibehålla förtroende hos våra samarbetspartners? Har vi tillräckliga åtgärder för att skydda vår organisation mot risker och intrång?

Tabell: Exempel på frågeställningar som bör finnas på bordet hos styrelsen, högsta ledningen och ägare.

Ledarskap och organisation - medvetenhet och förmåga att hantera cyber- och informationssäkerhet



6 Behoven av informationssäkerhetsarbete hos företagen

6.1 Vissa företag vinner mer på ett systematiskt arbete med informationssäkerhet

Företag som har mycket att vinna på ett ökat arbete med informationssäkerhet och på olika applikationsområden är exempelvis: tech startups, tillväxtbolag inom smart industri, tjänsteföretag som hanterar stora mängder data, e-handelsbolag, mjukvarubolag, teknikbolag inom IoT, molntjänster, mjukvara etc. Små och medelstora företag som ingår i djupare samarbeten med stora internationella företag med krav på anpassning av säkerhetsnivån drar samtidigt också fördelar av ett informationssäkerhetsarbete. Det handlar också om företag med mer avancerade affärsmodeller, som utvecklar digitala produkter och tjänster samt företag som delar data med andra i ett ekosystem av andra bolag och organisationer samt i leverantörskedjor.

Alla små och medelstora företag har behov av ett basskydd. Informationssäkerhet är naturligtvis ett ämne som bolagen diskuterar och som får allt mer uppmärksamhet. Samtidigt är det fortfarande en mindre andel av bolagen som verkligen arbetar strategiskt med informationssäkerhet - både för att skydda sig själva och som en strategisk konkurrensfördel.

6.2 Små och medelstora företag är ingen homogen grupp

Det är stor skillnad på digital mognad och krav på digitalt förändringsarbete mellan olika typer av företag, bl a baserat på affärsmodell och roll på marknaden. *European Digital SME Alliance* har gjort ett förslag till klassificering av företag i fyra grupper som alla har olika behov av lösningar och insatser.

Företagstyp	Digitalt beroende – många företag	Digital kärna	Digitalt baserad	Nystartat med tillväxtambitioner
Beskrivning	De flesta små och medelstora företag befinner sig i den här kategorin. Använder informations och kommunikationsteknologi (IKT) för att stödja sin verksamhet. Det kan t.ex. handla om ekonomisystem eller kundhanteringssystem eller enklare online-försäljning. Denna kategori har behov av lättförståeliga anvisningar, guider och praktiska lösningar.	I den här kategorin finns ett betydande antal små och medelstora företag som utvecklar och tillhandahåller digital hårdvara, mjukvara och tjänster.	Företag som har en digital affärsmodell som innebär att företaget utbyter data och information i ekosystem och leverantörskedjor. Dessa företag har ingen egen "digital produkt" eller "teknik" som sin kärnverksamhet, men är mycket beroende av digitala lösningar för sina affärsmodeller och huvudsakliga affärsfunktioner.	Nystartade företag, ofta fullt upptagna med utveckling av produkter, affärsmodeller, att få ombord de första kunderna eller hitta finansiering. Det leder lätt till att företagen försummar, eller inte känner till krav som "security by design".
Behov	• Kunna inventera vilken information som är mest kritisk. • Säkra den egna IT-miljön. • Efterleva externa lagar och krav. • Ställa krav på leverantörer. • Testa säkerheten. • Arbeta med att skapa en säkerhetskultur i företaget.	• Snabbt ökande behov av informationssäkerhet. • Ökande krav på kompetens och anpassning. Det handlar om allt från hur produkterna designas "security by design", till att följa industri-standarder och inneha nödvändiga certifieringar. • Stärka sin egen organisation med funktioner och ansvarsroller för säkerhetsfrågor och integritetsfrågor.	• Vara medveten om att ha kunskap för att i sin tur kunna ställa säkerhetskrav på sina leverantörer • Ha koll på att alla system och olika IT-plattformar de använder sig av och en hög säkerhet för personlig integritet.	• Skapa robusta och skalbara produkter som klarar industristandarder och regelverk när det gäller informationssäkerhet.

6.3 Några faktorer som ökar säkerhetsbehoven

För företagens ägare är säkerhet en strategisk fråga som i högsta grad påverkar företagets potential att växa samt företagets värde. Säkerheten i ett mindre företag blir extra viktig vid ett samarbete med ett stort internationellt företag, eller i samband med att ett företag vill ta in riskkapital och då en så kallad ”due diligence”, en kvalitetsundersökning görs av hela företaget där också en översyn av säkerhetsfrågor och relaterade branschstandarder ingår.

Vid en internationalisering gäller olika regelverk för säkerhet i USA, Asien och EU. För ett företag som utvecklar applikationer, exempelvis för videokonferenser eller spel, kan tillväxten ta snabba och oväntade riktningar, som leder till nya krav på anpassning av säkerhetsregler.

Figur: Faktorer som driver på komplexiteten inom informationssäkerhet

6.4 Både möjligheter och utmaningar för tillväxtbolagen

Digitaliseringen skapar fantastiska möjligheter för små och medelstora tillväxtbolag. För att nyttja den potentialen måste företaget ha förmågan att inkludera informationssäkerhetsperspektiven i företagets affärsutvecklingsprocesser. De företag som saknar insikter och kapacitet för att integrera säkerhet i sin verksamhetsutveckling kommer förr eller senare att möta tillväxthinder.

För att kunna utveckla nya tjänster, produkter och processer för den nationella och internationella marknaden behöver informationssäkerhet vara en integrerad del av verksamheten och affärsutvecklingen hos små och medelstora företag med tillväxtambitioner.

Stora företag, börsbolag och banker kan satsa avsevärda resurser på säkerhetsarbete, rekrytera och engagera de bästa experterna och leverantörerna inom säkerhet. De kan delta i internationella säkerhetssamarbeten och i arbetet att ta fram branschstandarder. Medarbetare håller sig uppdaterade i frågorna genom att delta i olika utbildningar och genom att erhålla olika certifieringar. Trots detta är säkerhetsfrågorna en ständig källa till oro hos styrelse och ledning hos de allra största företagen.

Digitaliseringen berör hela företaget, alla typer av affärer och processer från produktion till försäljning och marknad. För företag med mera avancerade affärsmodeller finns många strategiska vägval som kräver mera ingående kunskap, eftersom säkerhet är komplext och har flera specialistområden som *IoT* och *Cloud Security*, *Software Security*, *Communication (5G) Securitys*, samt *AI Based Security*. Dessa områden har dessutom ofta regelverk som är branschspecifika. Företagen behöver tänka strategiskt kring möjligheter och hot med användningen av data i ett ekosystem av olika aktörer. *Tredjepartsrisker,* se vidare sidan 15, innebär stora utmaningar för små och medelstora företag. En mängd frågor behöver hanteras av företagets styrelse och ledning, exempelvis:

- Vad är skyddsvärt, vilken typ av information och data är viktigast att skydda?
- Hur skapar vi konkurrensfördelar?
- Kostnader för informationssäkerhet – hur får vi tillbaka investeringar i intäkter?
- Vilka resurser och vilken kompetens behöver vi inom företaget?
- Vilka experter och partners ska vi välja att samarbeta med?

6.5 Bristande kompetens hos ägare, styrelse och ledning

Studier visar att styrelse- och strategiarbete rent generellt är en utmaning för det stora flertalet små och medelstora företag[5]. De flesta företag i denna kategori saknar ett professionellt styrelsearbete. Områden där det finns behov av att förstärka kompetens i styrelser är framförallt inom digitalisering, hållbarhet och internationalisering. Det faktum att det ser ut avspeglas naturligtvis på företagens förmåga att ta sig an säkerhetsarbetet.

Det finns inte en lösning som passar informationssäkerhetsarbetet i SMF. Det är ett av skälen till att säkerhet måste vara en prioriterad fråga för styrelse och ledning. I ett tillväxtföretag är styrelsens absolut viktigast uppgift att ha fokus framåt - att omvärldsbevaka, tolka och analysera omvärlden. Varje företag måste utarbeta en egen digital strategi som fungerar för varje enskilt fall och över tid.

För mindre företag är utmaningarna annorlunda än i storbolagen, men kan vara nog så stora. Här handlar det mer om prioriteringar eftersom dessa företag har begränsade resurser. Det finns också ett visst glapp mellan företagens behov/beställarkompetens och de tjänster som marknaden erbjuder. Det ställer därför höga krav på ägare och styrelse

[5] Strategisk styrelsekompetens, Rapport 0215, 2017, Tillväxtverket.

och att arbeta smart för att ta fram strategier och handlingsplaner som är anpassade efter både specifika behov och resurser.

Företagets värde finns i information

I många företag finns så mycket som 70–85 procent av företagets värde i information. Företagen ingår och är i ett slags beroendeställning i ett ekosystem av andra aktörer, ex vis företagskunder, samarbetspartner, leverantörer och myndigheter. Detta ställer extra krav på att också småföretagen har tillräcklig fokus på säkerhetsarbete. Vanligt är ansvaret delegerats till en särskild funktion, ofta IT-avdelningen eller en hosting-leverantör. I grunden saknas det insikter och rätt kompetens för att hantera informationssäkerhet rent företagsstrategiskt och ur ett konkurrens- och värdeskapande perspektiv. Det handlar om olika viljor och prioriteringar, till exempel hos företagets grundare, styrelse eller riskkapitalister.

Hos små företag är det ofta några få nyckelpersoner som sköter alla ledningsfunktioner. Man har inte resurser att bemanna alla funktioner på heltid. Medarbetare har därför ofta flera ansvarsroller. En person kan både vara marknads- och försäljningsansvarig och samtidigt också ansvara både för ekonomi och IT-frågor.

Ansvar och funktion

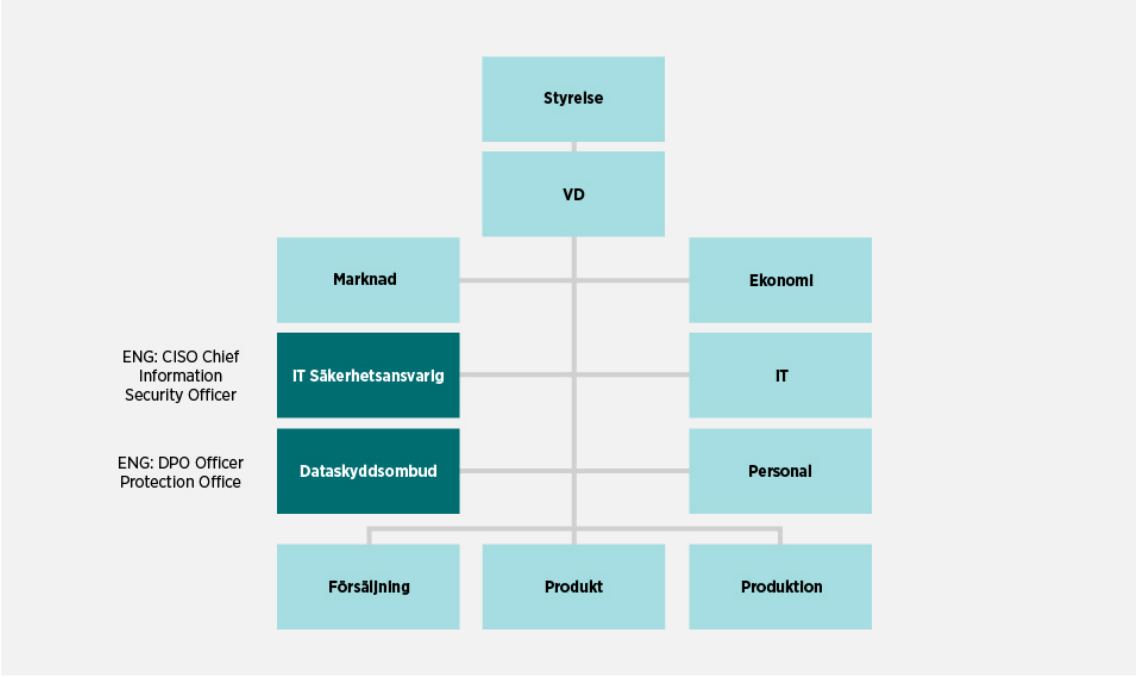
För att arbeta strategiskt och systematiskt med säkerhet och dataskydd är det avgörande att det finns utpekade ansvarsroller för dessa funktioner. Det räcker inte att placera ansvar för dessa områden hos till exempel en IT-ansvarig eller ekonomiansvarig person. Skälen är flera. Dels är både säkerhet och dataskydd komplexa frågor som behöver full fokus i hela företaget. Dels för att det är ansvarsområden som bör vara ”oberoende” till övriga organisationen och rapportera direkt till den verkställande direktören.

6.6 Alternativa sätt att arbeta med informationssäkerhet

För små och medelstora företag är det knappast ett alternativ, eller ett lagligt tvång, anställa en ansvarig för IT-säkerheten (eng. CISO, Chief information security officer), eller ett dataskyddsombud (eng. DPO, Data Protection Officer). Det gäller därför att hitta alternativa och nya sätt att komma igång med säkerhetsarbetet.

- Kanske finns någon i teamet med intresse och rätt bakgrund eller kan vi bemanna funktionen med en extern konsult under en uppstartsperiod?
- Vilken kompentens ska vi ha inom företaget?
- Kan vi dela en resurs med andra som vi samarbetar med?
- Vilken teknikplattform och delningsplattform passar bäst för oss?

För medelstora företag finns även alternativet att hyra in externa experter till säkerhetsavdelningen.



6.7 Att välja plattformar och säkerhetslösningar

För företag med tillväxtambitioner är det viktigt att tänka strategiskt från början, så att man väljer skalbara plattformar och säkerhetslösningar. Genom att använda standardlösningar och arbeta med ledande teknikplattformar, som till exempel Amazon Webservices, Google Cloud Platform, Microsoft Azure eller Huawei, har företaget tillgång till en enorm utvecklingskraft, olika expertforum, certifieringar och djupgående lösningar för olika branscher. Det är omöjligt att kunna allt inom ett företag - det är en så stor bredd av frågor. Det kan handla om kryptering, användning av kameror, lagar, regler och avtal. Det är därför viktigt att omge sig med experter och att ingå i branschnätverk och forum för att hitta aktuell kunskap.

6.8 Det saknas säkerhetsstandarder anpassade för mindre företag

Det är viktigt att ha rätt säkerhetsstandard på produkter för att hålla samma säkerhetsnivå som kunder och samarbetspartner. Detta är en utmaning eftersom komplexiteten är hög och standarderna inte är anpassade för mindre företag i tillräckligt hög grad. De små företagen kan utgå från modeller som används av större företag och skala ned och anpassa verktygen till ett mindre företags förutsättningar. Exempel på sådana ramverk är *NIST (National Institute of Standards and Technology)* och *CIS (Center for Information Security).*

6.9 Svårt välja rätt partner och leverantörer inom säkerhet

Att hitta rätt nätverkspartner, konsulter och leverantörer inom säkerhet är inte helt enkelt för mindre företag. Framförallt när det gäller strategisk säkerhet och mera djupgående expertis samt experter som både kan säkerhet, företagande och affärsutveckling.

Det finns ett relativt bra utbud av IT-konsultföretag som kan hjälpa företag med ett basskydd inom IT-säkerhet. Andra ka behöva ta in expertkonsulter och expertföretag inom säkerhet. Eftersom storbolagens efterfrågan på säkerhetsexperter är hög, och då det råder en generell brist på marknaden, är de flesta säkerhetsexpertföretag inriktade på lösningar för större bolag. Efterfrågan driver också på prisbilden på spetskompetens.

Det finns ett glapp i marknaden vad gäller erbjudanden, resurser och beställarkompetens. Små tillväxtföretag som ofta inte ens har egen IT-kompetens, får hitta andra sätt bemanna, hyra in eller dela resurser.

6.10 Vägledning och råd för småföretag

MSB

För att möta ett grundläggande behov hos medborgare och små företag, finns ett antal guider och vägledningar från bland annat Myndigheten för samhällsskydd och beredskap, MSB.

I oktober varje år arrangeras *Tänk säkert-kampanjen* i samarbete med en rad myndigheter och olika intresseorganisationer. Kampanjen vänder sig till allmänheten, det vill säga privatpersoner och de allra minsta företagen, läs mer på www.msb.se/tanksakert

För målgruppen små företag finns även att antal guider och skrifter[6], exempelvis:

- Informationssäkerhet för små företag (2018).
- Skydda din dator och mobiltelefon.
- Skydda din företagsinformation.
- Skydda ditt företag mot bedrägerier.
- Upphandla informationssäkert (2018).
- Grundläggande IT-säkerhetsåtgärder (2019).

Andra källor och guider

Andra källor som små företag och allmänheten kan vända sig till är till exempel: Svenskt näringsliv – Näringslivets säkerhetsdelegation, Stöldskyddsföreningen (SSF cybersäkerhet bas), Teknikföretagen, banker och försäkringsbolag samt företagarföreningar och branschförbund. Teknikföretagen exempelvis har några poddavsnitt om cybersäkerhet och den ökade hotbilden mot Sverige.

Tillväxtverket genomförde under maj 2020 ett webbsänt seminarium med syftet att öka kunskapen om informationssäkerhet - som utmaning och möjlighet för digitala affärer. Filmerna går att se på Tillväxtverkets Youtube-kanal.

Under sommaren 2020 publicerade Teknikföretagen en guide till medvetet säkerhetsarbete i mindre teknikföretag ”Skydda din IT-miljö” och också en publikation om cyberhoten mot svenska teknikföretag.

[6] www.informationssakerhet.se

6.11 Utbudet av utbildningar inom cybersäkerhet

Det finns en hel del kurser och utbildningar. SFF Cybersäkerhet bas, Certifiering enligt ISO/IEC 27001:2017, NIST Cyber Security Framework, m.m. På ledningsnivå har exempelvis KTH Executive School en utbildning mot ”Strategic Cyber Security”. Men många utbildningar på både den privata och offentliga marknaden är i form av korta seminarier eller e-utbildningar. Det är svårt att hitta utbildningar som går mera på djupet, som fångar och engagerar deltagarna och ger ”hands on” träning med riktiga fall från det egna företaget.

7 Den digitala hotbilden

Varje sekund flödar 77 terabyte av internettrafik. Internet underlättar nästan alla aspekter av det moderna samhället, och för affärer kan det liknas med vad Sidenvägen hade för funktion som pulsåder för handel under medeltiden. Precis som forntida köpmän plågades av banditer på resan längs Sidenvägen, kan dagens entreprenörer, när de minst anar det, befinna sig under attack från någon form av IT-relaterad brottslighet. Det gäller inte minst små och medelstora företag. Denna kategori står för 43 procent av alla incidenter, enligt en rapport *från Verizon (2019*).

Samhällets mörka sidor har sedan länge flyttat ut på nätet. Det är helt enkelt billigare, säkrare och enklare än att begå konventionella brott som att råna banker. Utvecklingen är mycket snabb och det kommer ständigt nya tekniker och metoder. Sex av tio svenskar är oroliga för att drabbas av en IT-attack. 41 procent har redan utsatts för någon form av dataintrång, privat eller på jobbet (*Sentor 2017*).

Några exempel på siffror som illustrerar hotbilden:

- 100 000 cyberattacker mot Sverige varje år
- 10 000 anmälda kortbedrägerier på internet varje månad
- 400 000 mobila enheter med virus eller skadliga program
- 17 000 datorer med virus eller skadliga program
- 50 allvarliga incidenter på ett år
- 50 procent av Sveriges företag saknar resurser för att klara en attack

Källa: FRA, CERT-CE, NBC POLISEN, MCAFFE, PTS och NTT SECURITY

Cyberhot förekommer på många nivåer och i olika grad av organiserad verksamhet. Allt från *enskilda hackers* (Lone Wolfs), till intressegrupper, politiska, religiösa eller andra intressen och mer eller mindre extrema *hacktivister* (aktivistgrupper på nätet), företagsspioner, cyberspioner, organiserad brottslighet, terroristorganisationer eller statsunderstödda hacktvister på nationell nivå.

De största cyberhoten mot verksamheten i svenska bolag är den ovetande medarbetaren 64%, organiserad brottslighet 51% och hacktivisthotet 36%.

Källa: PWC Nordic Cyber Crime Survey 2020

Hackarna har gått hand i hand med IT-utvecklingen och blivit allt mer sofistikerade. Dagens hackare är ofta professionella kriminella, och även om alla har sin egen profil så finns det ett par grundläggande typer som är bra att känna till. Att förstå olika grupper av hackare – vad som motiverar dem och vilka metoder de använder – kan vara en hjälp för

att identifiera potentiella risker. Enligt Roger A Grimes, cybersäkerhetsexpert finns tio grundläggande hackartyper, se vidare artikel från 2019[7].

När olika system i världen kopplas upp och samman via nätet ökar exponeringen av den transporterade informationen. Detta sker kontinuerligt när användare, anslutna system och mängden information ökar. Därmed ändrar hoten mot systemen karaktär.

Attacker kan vara *riktade* eller *oriktade.* Exempel på riktade attacker är att företag kartläggs i ett visst syfte och ibland under en längre tid, så kallat cyberspionage, stöld av information eller ekonomiska resurser och på individnivå så kallad nätfiske (spear phishing) där riktade mejl skickas ut till enskilda personer.

Vid oriktade attacker söker hackare på nätet efter sårbara mål, till exempel ej uppdaterade programvaror i datorer, svaga lösenord eller genom nätfiske av mejl där man försöker komma över känslig information om till exempel kort- och kontouppgifter.

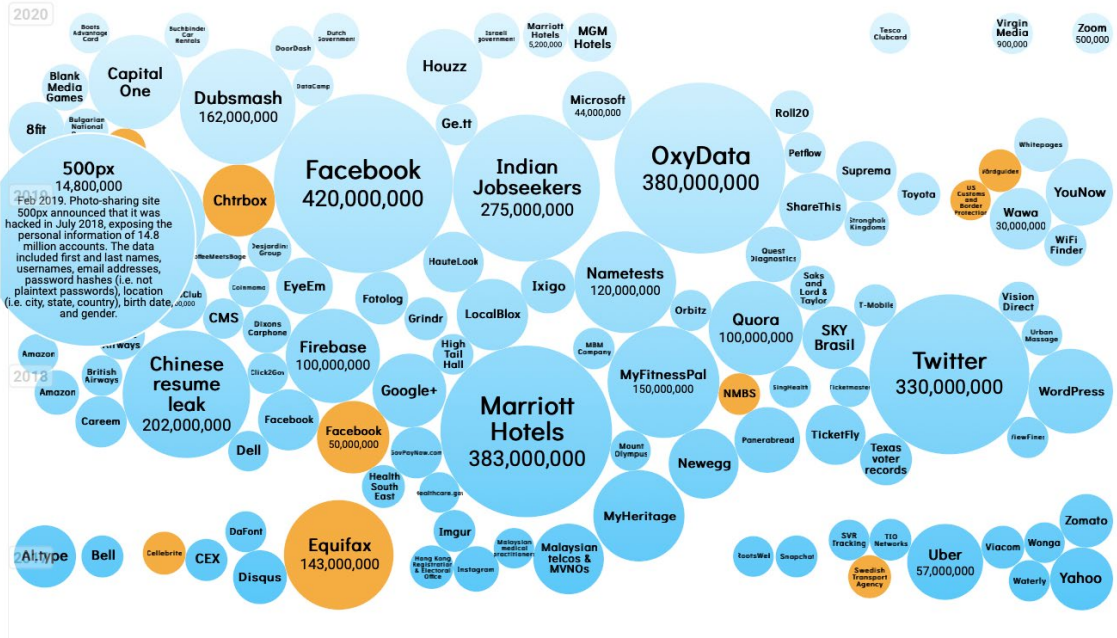
Exempel på olika typer av cyberattacker

- skadlig kod (eng. *malware*) till exempel virus, maskar, trojanska hästar
- utpressningsprogram eller gisslanprogram (eng. *ransomware*) - när filer krypteras och ägaren krävs på en lösensumma för att filerna ska dekrypteras
- överbelastningsattacker
- attacker genom nätfiske (eng. *phishing)* - användare luras att fylla i kort- eller kontouppgifter på falska webbsidor
- ID-kapning
- företagskapning

[7] Källa: Techworld, IDG, artikel 2019-03-17

8 Cyberbrott - skador för företag och samhälle

Vad har Equifax, Yahoo och den amerikanska militären gemensamt? De har alla fallit offer för en cyberattack någon gång under det senaste decenniet - och de är bara toppen av isberget. Mellan 2019–2023 kommer cirka 5,2 biljoner dollar[8] i globalt värde att vara i fara för cyberattacker, vilket skapar en enorm utmaning för både företag och investerare.



Figuren ovan illustrerar de största intrången i världen under de senaste tre åren.

Källa: Informationbeautiful, World biggest data breaches 2018—2020.

Under senare år har det skett omfattande och upprepade angrepp mot svenska företag för att stjäla eller förstöra digital information och system. Det gör att behovet av informationssäkerhet i allmänhet och cybersäkerhet i synnerhet växer.

> ”Allt som allt handlar det om fler än 100 000 cyberattacker per år i Sverige vilket skapar en totalkostnad på cirka 16 miljarder kronor hos svenska företag.”
>
> *Patrik Sandgren, Teknikföretagen*

Exempel på effekter av skador som företag kan drabbas av är informationsförluster, avbrott i verksamheten, försämrad leveransförmåga, tappad orderingång, förlorat

[8] Källa: World Economic Forum, 2019

förtroende hos och förlust av kunder, färre nya kunder eller bristande efterlevnad av rättsliga krav.

8.1 Småföretag - svårt att återhämta sig efter en större cyberattack

Små och medelstora företag förlitar sig alltmer på nätverk och informationssystem för sin verksamhet. Vissa av dem erbjuder tjänster där deras affärsmodell baseras på digital teknik. Samtidigt är små företag hårt exponerade för risker, och har svårare att återhämta sig från skador orsakade av en cyberattack, än stora företag. Enligt *European Digital SME Alliance* är det så illa att 60 procent av de små och medelstora företagen som varit offer för cyberattacker inte klarar att återhämta sig, utan måste avveckla verksamheten inom ett halvår efter attacken.

Norsk Hydro: Cyberattacken kostar en halv miljard

Cyberattacken mot den norska aluminiumjätten Norsk Hydro kommer att kosta bolaget mellan 400 och 450 miljoner norska kronor. Det uppger bolaget i ett pressmeddelande.

I mitten av mars 2019 utsattes företaget för ett omfattande cyberangrepp. Attacken resulterade i att enskilda verksamheter stoppades helt, medan andra fick ställas om i manuellt läge. Framför allt tvingades bolaget stoppa tillverkningen av specialtillverkade (extruderade) produkter i högautomatiserade fabriker.

”Cyberattacken som slog mot oss den 19 mars påverkade hela vår globala organisation, där verksamhetsområdet ”Extruded Solutions” blev hårdast drabbat, både vad gäller driftsproblem och finansiellt tapp”, säger bolagets vd Svein Richard Brandtzæg, enligt ett pressmeddelande. Med anledning av cyberattacken har bolaget valt att skjuta på kvartalsrapporten till den 5 juni.

Källa: Dagens Industri, 30 april 2019

8.2 God säkerhetskultur ökar konkurrenskraften

God säkerhet och tillit till företagens it- och säkerhetsarbete i organisation, processer, produkter och tjänster ökar konkurrenskraften. Allt mer komplexa nätverk och ett ökat beroende av nätverksbaserade tjänster inom alla delar av samhället ökar kraven på säkerhet och kvalitet. Idag använder vi internet mer än någonsin. Men detta är i grunden inte säkrare än i början av 1990-talet. Avgörande för all informationshantering, oavsett om det sker via internet eller på annat sätt, är tillgänglighet till systemen.

Det måste finnas ett förtroende för att

- informationen är korrekt, inte kan förstöras och inte röjas,
- rätt och behörig person skickar informationen,
- rätt och behörig person tar del av informationen.

En god säkerhetskultur kräver robusta IT-system och en allmän tillgång till säkerhetslösningar som innefattar möjligheter att

- identifiera aktörer på ett säkert sätt,
- skapa elektroniska signaturer,
- skydda informationen med hjälp av kryptering, exempelvis för e-mejl
- säkra att data inte försvinner – mycket känslig data och information bör dessutom förvaras fysiskt.

9 Marknaden för cybersäkerhet

Cybersäkerhetsmarknaden värderades till 116 miljarder USD[9] under år 2018 och förväntas nå 261 miljarder USD år 2024, med en årlig på tillväxt på 14 procent. Privata näringslivet, finansiella sektorer och banktjänster har utsatts för cyberattacker värda ett par miljarder dollar under de senaste åren. Dessutom har det expanderande trådlösa nätverket för mobila enheter ökat datasårbarheten. Behoven av cybersäkerhetslösningar förväntas växa globalt, inte minst i Asien och Stillahavsområdet.

De viktigaste drivkrafterna för en ökad efterfrågan av cybersäkerhetslösningar är

- den ökade tillgången på digitala lösningar och sjunkande priser. Användbarheten prioriteras dock ibland före säkerheten. Leverantörer av digitaliseringslösningar måste kunna hantera säkerheten.

- de ökade cyberhoten och ett ökat antal rapporterade cybersäkerhetsincidenter. Mörkertalet i antalet incidenter framför allt hos företag är fortfarande stort.

- den ökande regleringen kring datasekretess

- det ökande antalet datacenter

- den ökade medvetenheten om cybersäkerhet hos små och medelstora företag och organisationer som driver på efterfrågan och utvecklingen av nya cybersäkerhetslösningar. Nämnas kan bl. a framväxten av företag som erbjuder tjänster inom etisk hacking (lagliga penetrationstester av säkerheten) Samtidigt finns det fortfarande en bristande medvetenhet hos många företag om riskerna - exempelvis med piratkopierade cybersäkerhetslösningar.

9.1 Ökad tillväxt cybersäkerhetslösningar särskilt inom vissa sektorer och branscher

Efterfrågan på försvars- och myndighetsorienterade applikationer drev på marknaden under år 2018. Tillväxten hänger ihop med allt högre kostnader för säkerhetslösningar och en växande oro för dataintrång i underrättelse-, forsknings- och utvecklingsaktiviteter samt i finansiella aktiviteter. Denna kan potentiellt leda till cyberterrorism.

Banksektorn, men även finans- och försäkringsbranschen efterfrågar allt mer cybersäkerhetslösningar och expertis inom området på grund av den ökade cyberbrottsaktiviteten. Bank, finans och försäkringssektorn är ryggraden i samhällsekonomi och infrastruktur. Säkerhet är och måste vara mycket högt prioriterad. Som svar på de växande hoten och överträdelserna ökar regeringar över hela världen sina utgifter för att bygga och utveckla infrastruktur med hög cybersäkerhet. Andra större tillämpningsområden är hälsovård, IT och telekommunikation, bilindustri och handel.

[9] Allied Market Research, 2018.

Det finns ett antal tydliga segment i marknaden där företagen har olika erbjudanden, produkter och tjänster. Dessa segment är: företagslösningar, användarutrustning (desk-top, lap-top, mobil), molntjänster, nätverk och applikationer/programvaror. Det finns i sin tur lösningar för specifika funktioner som till exempel Unified Treat Management (UTM), Data Loss Prevention (DPM), Identity and Access Managment (IAM), Security information and Event Management (SIEM), Distributed Denial of Service (DDoS) och Risk & Compliance.

9.2 Trender och framtiden

Världen är mer uppkopplad än någonsin. Vi blir mer tekniskt avancerade, marknaderna är starkare och digitala lösningar som stöd för vårt dagliga liv växer ständigt.

Våra data delas och används nu av fler plattformar än någonsin: i datacenter, i molnet och via Internet of Things, IoT-enheter. Denna trend kommer bara att öka. Men till de stora fördelar och mervärden som tekniken skapar för människan, kommer också en kostnad i form av en ökad sårbarhet både för företag som på ett mer personligt plan.

En rapport från *Word Economic Forum (2019*) förutspår vad som sannolikt kommer att hända i cyberlandskapet under de kommande åren. Rapporten pekar ut fem områden.

"Kalla kriget" på nätet intensifieras

Ett nytt ”kallt krig" äger rum på nätet när västerländska och östliga makter i allt högre grad ”separerar teknik och nätverk”. Den pågående handelskonflikten mellan USA och Kina, och frikopplingen av dessa två ekonomier är ett tydligt tecken på detta. Cyberattacker kommer i allt högre grad att användas som s.k. proxykonflikter mellan mindre länder - finansierade, styrda och möjliggjorda av andra och större länder som vill konsolidera och utvidga sitt inflytande runt om i världen.

Dessutom fortsätter kritisk och för samhället viktig infrastruktur att vara en måltavla för cyberattacker, exempel finns i attacker mot amerikanska och sydafrikanska energiföretag i år. Nationer måste allt mer stärka sitt cyberförsvar av sin kritiska infrastruktur.

Framväxten av artificiell intelligens, AI – samma teknik möjliggör både cyberbrott och cybersäkerhetslösningar

Under USA:s val år 2016 spreds AI-baserade falska nyheter, *faked news*, för att undergräva motståndarnas trovärdighet. Det är varken första eller sista gången som politiska kampanjer kommer att drivas på detta sätt. AI-tekniken är en möjliggörare cyberbrott, exempelvis genom skadlig programvara. Samtidigt kan samma teknik användas för att utveckla säkerhetsåtgärder för att stoppa brott och skadeverkningar. AI påskyndar identifieringen av nya hot vilket underlättar blockeringar av attacker innan de når bredare. De flesta säkerhetslösningar är i nuläget baserade på sk upptäcktsmotorer som bygger på en mänskligt skapad logik. Det gäller att hålla teknik och enheter ständigt uppdaterade.

Kommunikationsverktyg och sociala medier måltavlor för cyberattacker

Den ökade uppkopplingen skapar nya slagfält. Under första halvåret 2019 såg vi en 50 procentig ökning av skadliga programvaror riktade mot hanteringen av mobila bankärenden jämfört med förra året. Våra betalningsuppgifter, referenser och pengar kan lätt hamna hos kriminella efter en cyberattack. Cyberbrott genom försök att lura till sig personuppgifter ökar Attackerna kommer att gå från traditionell e-post till attacker via

sms, sociala medier och spelplattformar. Vanliga kommunikationsmedel kan bli ännu populärare attackytor.

5G-utveckling och tillväxten av IoT-enheter ökar sårbarheten

När 5G-nät lanseras kommer användningen av anslutna IoT-enheter att påskyndas dramatiskt och massivt öka nätverkens sårbarhet för storskaliga cyberattacker. IoT-enheter och deras anslutningar till nätverk och moln är fortfarande en svag länk inom säkerhet. En ständigt växande volym av data och personuppgifter kommer att behöva säkras mot brott och stöld. Vi behöver mer av en helhetssyn på IoT-säkerhet och vi behöver kombinera traditionella och nya metoder för att hantera dessa snabbt växande nätverk med massiv kapacitet att generera data.

Företag kommer att tänka om i sin molnstrategi

Att identifiera olovlig aktivitet i systemen räcker inte längre för att säkerställa skydd. Förebyggande aktiviteter är nyckeln till att vara säker. Många organisationer kör redan en de flesta av sina applikationer i molnet, men förståelsen för säkerhet i molnet är fortfarande låg. Säkerhetslösningar måste utvecklas för nya, flexibla, molnbaserade arkitekturer som ger skalbart skydd med snabbhet.

9.3 Vad kommer härnäst?

Det går knappast en dag utan att en incident av ett intrång eller en cyberhändelse rapporteras in till Myndigheten för samhällsskydd och beredskap, MSB. Statliga myndigheter ska rapportera in IT-incidenter och störningar till MSB. Krav på incidentrapportering gäller också för leverantörer av samhällsviktiga tjänster.

Attacker har blivit så pass vanliga skadliga att amerikanska FBI delvis ändrat sin inställning till att betala lösensummor. Byrån anser nu att företag i vissa fall kan behöva överväga att betala för att skydda sina aktieägare, anställda och kunder. Genom en analysprogramvara kan det konstateras att det sker nästan 90 miljarder försök till intrång per dag - jämfört med uppskattningsvis 6 miljarder dagliga sökningar på Google. Genom att förstå hotbilden kan vi förbereda oss bättre. Den enorma spridningen av teknik och lösningar kommer att tvinga oss till bättre kraftsamlingar. Cyberattacker inte längre är en fråga om, utan när och hur. Detta är ett hot och en oro som påverkar oss alla.

10 Slutsatser och rekommendationer

Informationssäkerhet har fått mera fokus under senare år både på EU- och nationell nivå. 2018 presenterade regeringen en nationell strategi för samhällets informations- och cybersäkerhet. Samma år gav regeringen Myndigheten för samhällsskydd och beredskap, MSB, i uppdrag att öka allmänhetens samt småföretagens - med särskilt fokus också på mikroföretag - kunskap om informationssäkerhet. Regeringen gav hösten 2019 Försvarets radioanstalt, Försvarsmakten, MSB och Säkerhetspolisen i uppdrag att förbereda inrättandet av ett nationellt cybersäkerhetscenter under 2020. Det nationella cybersäkerhetscentret ska stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige och minska cybersårbarheterna.

Digitalisering och informationssäkerhet går i högsta grad hand i hand. Att som litet företag bli utsatt för en cyberattack är idag en reell risk som behöver tas på största allvar. De största tillgångarna och värdet hos många företag finns idag dessutom i företagens data och information. På samma sätt som att en framgångsrik digitalisering kräver ett framsynt ledarskap så gäller detta i ännu högre grad för informations- och cybersäkerhet.

Digitaliseringen skapar fantastiska möjligheter för små och medelstora tillväxtbolag. För att nyttja den potentialen måste företaget ha förmågan att inkludera informationssäkerhetsperspektiven i företagets ordinarie utvecklingsprocesser. De företag som saknar insikter och kapacitet för att integrera säkerhet i sin affärs-, verksamhets-, process- och produktutveckling kommer förr eller senare att möta tillväxthinder.

Tillväxtföretagen ingår idag i ekosystem där stora och små företag delar data och information. Detta kräver att företagen håller samma säkerhetsnivå i systemen för att kunna delta. För de företag som vill göra med affärer med stora företagen gäller särskilda säkerhetskrav, standarder och regelverk som de stora företagen själva etablerat.

Informationssäkerhet och cybersäkerhet är ett komplext område för små och medelstora företag. Rent generellt kräver det att företaget redan har ett väl fungerade strategiarbete på plats. För företag med mera avancerade affärsmodeller är säkerhet ett komplext område i ständig utveckling. Det sätter företagen inför många utmaningar.

Cyberhoten och antalet IT-incidenter har ökat dramatiskt de senaste fem åren. Samtidigt driver teknikutvecklingen med IoT, AI och nästa generations mobila kommunikation (5G) på mot allt mera komplexa nätverk och ett ökat beroende av nätverksbaserade tjänster inom alla delar av samhället. Detta ökar kraven på säkerhet och kvalitet.

Insikter och kunskap inom informations- och cybersäkerhet på strategisk nivå är avgörande för att små och medelstora företag ska kunna växa hållbart. Säkerhetsfrågorna har ofta inte en tillräcklig prioritering hos ägare och styrelse. För att ta sig an säkerhetsarbetet med begränsade resurser och grundkompetenser behöver man arbeta smart och testa olika vägar framåt som fungerar för det egna företaget. Det är dessutom en generell brist på spetskompetens inom säkerhetsområdet på marknaden. Större delen av utbudet av säkerhetstjänster är riktade mot större företag. Det gäller därför att hitta alternativa och nya sätt att komma igång med säkerhetsarbetet.

10.1 Förslag på kompetenshöjande åtgärder

För målgruppen små och medelstora företag finns flera bra initiativ, t.ex. genom Myndigheten för samhällsskydd och beredskap, MSB, och olika branschorganisationer

som arbetar med att höja baskunskaperna inom informations- och cybersäkerhet genom inspirations-, insiktsarbete, vägledningar och guider.

Behoven av att höja kunskapen hos ledning och styrelse är fortsatt stort. Bristande grundkunskaper inom området riskerar bli en barriär för svenska små och medelstora företags tillväxt. Det finns även brister i marknadens utbud av kompetens och tjänster som är nivå- och målgruppsanpassade för små och medelstora företags behov.

Nedan presenteras några förslag på kunskapshöjande insatser inom några områden:

Roadmaps, ramverk och verktyg anpassade för olika små och medelstora företags behov, även med branschfokus

Roadmaps

För olika tillämpningsområden inom Internet of Things, IoT, finns bra exempel från England där *IoT Security Foundation* tagit fram mycket konkreta ”roadmaps” för företag med vägledning inom olika områden. I Sverige har IoT Sweden (Strategiskt informationsprogram SIP) noterat en ökad efterfrågan av säkerhet, och betraktar det arbete som görs inom IoT Security Foundation som mycket inspirerande.

Konkreta vägledningar för mjukvarubolag

För nystartade företag med tillväxtambitioner finns exempel från Silicon Valley på vägledningar för vad ett startup-bolag behöver tänka på. Riskkapitalbolaget *Bessemer Venture Partners* har tagit fram en mycket konkret guide på temat ”The affordable ten-step plan for survival in cyberspace”. Denna vägledning går på djupet och har konkreta råd, exempelvis vid rekryteringar styrelseledamöter, för att skapa en säkerhetskultur, för att använda och upphandla tekniska plattformar. Det finns också konkreta råd och tips för hantering av epostsystem, kravställning på hemsidor, brandväggar, nätverk, hur man skapar en beredskapsplan, hanterar ekonomiska och juridiska risker, fysisk infrastruktur samt hur programmerare kan tänka för att producera ”säker kod”. Denna typ av konkreta vägledningar kan utvecklas för olika typer av tillväxtbolag (”*digitala möjliggörare*”, ”*digitalt beroende*”).

Ledningsverktyg

Det finns väl utvecklade ramverk för stora företag för styrning och uppföljning av sitt arbete med informationssäkerhet. Ett exempel är ett ramverk *NIST, National Institute of Standards and Technology*, som publicerar standarder och riktlinjer för informationsteknologi. Med NIST-ramverket kan ett företag få en bild över sin ”säkerhetsprofil” och även jämföra sig med best practices.

Ett annat ramverk, *CIS, Center for Information Security*, är en amerikansk organisation som specialiserar sig inom informationssäkerhet. CIS ger ut en samling av säkerhetsrekommendationer (20 kontrollpunkter). Organisationen arbetar sedan sin start tillsammans med amerikanska myndigheter och företag för att ta fram arbetsmetoder med målet att höja säkerhetsnivån och medvetenheten inom IT-säkerhet. CIS kontrollverktyg, idag standard inom IT-säkerhet, och analyser är anpassade för att kunna användas vid ”Due Diligence”, för utvärderingar och kontroll inför uppköp eller sammanslagningar av företag. Denna typ av verktyg skulle kunna utvecklas och användas också för det mindre företagets behov.

Skapa tillgängliga ”sandlådor” för cybersäkerhet

Ett annat område av intresse handlar om att skapa cybersäkerhetsprogram med ”sandlådor” (eng. *sandbox*) för innovation och informationssäkerhet utformade för att stötta små företag eller tillväxtföretag när de utvecklar innovativa produkter och tjänster. En sådan kan också inspireras av *Information Commissioner's Office, ICOb*, i Storbritannien som öppnat en ny tjänst för att stödja organisationer som använder personuppgifter för sin verksamhet. Detta för att utveckla produkter och tjänster som är innovativa och som tas fram och används på ett för allmänheten korrekt sätt.

Kompetensinsatser för främjarsystemen – insikter och kunskap

Med undantag för några få spetsinkubatorer och innovationsmiljöer är kunskapen inom informationssäkerhet och cybersäkerhet låg inom främjarsystemen. Det finns därför behov av riktade och nivåanpassade insatser för olika typer av främjare, sk ”train-the-trainer”-insats. Då säkerhet är ett komplext ämne finns det anledning att tänka nytt.

Expertrådgivare inom säkerhet kan beredas möjlighet att ta delta i utbildningar och ta del av den senaste kunskapen genom att delta i olika säkerhetsforum, t ex InfoSecurityForum.

Informationssäkerhet en förutsättning för hållbarhetsarbete, dvs för att utveckla sunda och livskraftiga företag. Det är därför naturligt att företagsfrämjare lyfter in informationssäkerhet som ett kriterium och krav i sina affärsutvecklingsprocesser på samma sätt som andra hållbarhetskriterier.

Cyberförsäkringar

Ett annat område där främjarsystemet kan spela en roll är för att informera om cyberförsäkringar. Cyberförsäkringar är relativt okända hos små tillväxtföretag. En cyberförsäkring kan aldrig ersätta en god riskhantering i en verksamhet, men försäkringen kan kapa toppen av kostnaderna för cyberskador.

Konsultcheckar till företag för strategiskt informationssäkerhetsarbete

Ett sätt att öka insikter och minska trösklar är att kunna erbjuda särskilda konsultchecker för strategisk informationssäkerhet. Ett användningsområde för checkarna skulle kunna vara för att genomföra stresstester och simuleringar av intrång (penetrationstester).

Pilotinsatser för lärande och djupkunskap om behoven hos olika målgrupper av företag

Det kan konstateras att små och medelstora tillväxtföretag inte är en homogen grupp. Gruppen av företag har olika utmaningar att ta sig an området *strategisk informationssäkerhet.* Det finns ett glapp i marknaden mellan företagens behov och den paketering av tjänster som marknaden erbjuder. De mindre företagen har behov både på styrelse- och ägarnivå som i ledningen och organisationen för ett strategiskt förändringsarbete med fokus på mer operativt säkerhetsarbetet. Företagen har ofta svårt att prioritera insatser som inte uppfattas ger snabb återbetalning av investerade medel. Pilotinsatserna kan därför även fokusera på att lyfta fram förebilder och goda exempel

Vi behöver mer och bättre kunskap om olika typer av företags faktiska behov av säkerhet samt hur, i vilket format, med vilka angreppsätt samt i vilka sammanhang de ser att det är mest meningsfullt att engagera sig i detta förändringsarbete.

Pilotinsatser för juridik/lagstiftning kopplat till cybersäkerhet

Juridiken bör tas med från början i digitaliseringsprojekt så att den blir ett stöd istället för ett hinder. Juridiska frågeställningar behöver finnas med när olika digitala system upphandlas, utvecklas och designas eftersom kostnaderna för juridiska tjänster annars riskerar att bli högre senare i processen. Information och data står ju idag för den största värdet i många företag.

I takt med att företag kopplar upp sig i ekosystem och utbyter information ökar behovet att skydda sina tillgångar. Det gäller både för säker teknik och genom affärsjuridiska avtal.

Det finns även områden där det finns lagstiftning att efterleva, t ex kring GDPR. Den snabba teknikutvecklingen ligger tidvis före lagstiftningen och det kan vara svårt att tolka regelverk och lagstiftning. För tillväxtföretag finns därför en extra koppling mellan informationssäkerhet och juridik.

Då det finns glapp i marknaden för små och medelstora företag att hitta rätt juridisk kompetens finns ett värde av att ta fram mera kunskap om hur processer och arbetssätt kan organiseras i för att hitta ett bra gränssnitt där kompetens inom informationssäkerhet och affärsjuridik kan samspela på ett sätt som passar behoven hos företagen i målgruppen.

Bilaga 1 - Ökad reglering på nationell och internationell nivå

Enskilda företag eller nationer kommer inte själva att klara av att hantera alla dimensioner av cybersäkerhet. Tvärtom så efterfrågas och välkomnas flera initiativ av ökad reglering. Jämfört med de flesta andra samhällskritiska områden, är informationssäkerhet inte ett område omgivet av starka regleringar, varken på nationell eller på internationell nivå. Internationellt gäller dessutom olika regelverk och standarder i Asien, USA och Europa.

Under de senaste åren har det tillkommit ett flertal nya regelverk. Exempel på regelverk är GDPR, kameraövervakningslagen, NIS-lagen, säkerhetsskyddslagen, CLOUD Act och EU Cyber Security Act.

Nedan ges kort beskrivning av ett urval av regleringar på EU-nivå och nationell nivå:

Dataskyddsförordningen (GDPR)

Dataskyddsförordningen, GDPR (The General Data Protection Regulation), gäller i hela EU och har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter, så att det fria flödet av uppgifter inom Europa inte hindras. Ett av syftena med dataskyddsförordningen är att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Rätten till privatliv uttrycks i den Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR). I artikel 8 ges rättighet till respekt för privat- och familjeliv, hem och korrespondens. Konventionen har införts som lag i Sverige. Även i EU:s stadga om grundläggande rättigheter uttrycks rätten till respekt för privat- och familjeliv, i artikel 7. Här finns också en särskild bestämmelse om rätt till skydd av personuppgifter, i artikel 8. Stadgan är rättsligt bindande för EU:s medlemsstater. På svensk nivå finns en grundlagsstadgad rätt till skydd för den personliga integriteten i samband med behandling av personuppgifter, i 2 kap. 6 § andra stycket regeringsformen.

Cybersecurity Act – EU:s väg mot ett säkrare moln

EU:s nya förordning **Cybersecurity Ac**t (*2019/881*) antogs 17 april 2019 och upphävde därmed den tidigare förordningen *(EU) nr 526/2013.* Syftet med Cybersecurity Act är att bidra till en enhetlig säkerhetsnivå och standard i EU. Den innebär ett utökat mandat för ENISA (Europeiska unionens cybersäkerhetsbyrå) och den skapar ett europeiskt certifieringsramverk för IKT-produkter, tjänster och processer. Certifieringen kommer att erbjudas i tre olika nivåer och kommer, åtminstone initialt, att vara frivillig både för företag inom och utanför EU.

CSP Cert[10] har sedan verksamheten bildades år 2017 haft i uppdrag att föreslå omfattning och nivå på ett certifieringsramverk för molnaktörer i enlighet med Cybersecurity Act. I likhet med övriga certifieringar under förordningen, kommer molncertifieringen, åtminstone initialt, att vara frivillig.

SWIPO (Switching and Porting, Code of Conduct Group) arbetar med att utveckla ”best practice” och informationskrav på EU-nivå, såsom definierat i EU-kommissionens förslag

[10] https://www.cert.se/ (MSB)

på fritt flöde av icke-personliga uppgifter (artikel 6), för att underlätta byte av molnleverantör och förhindra ”vendor lock-in”*. Cybersecurity Act är aktuellt för både leverantörer och kunder, och kan komma att bli en viktig del i kravställningar inom upphandling och inköp.

* innebär att en kund blir låst i en relation till en relation med en leverantör av en tjänst eller vara, exempelvis molntjänster.

Vad kan EU:s Cybersecurity Act innebära för små och medelstora företag?

Små och medelstora företag spelar en viktig roll för att tillhandahålla cybersäkerhetslösningar. Ett nyligen publicerat dokument från europeiska cybersäkerhetsorganisationen (ECSO) uppskattar att

60 000 företag - varav 98 procent är små och medelstora företag och nystartade företag - är aktiva på EU: s cybersäkerhetsmarknad. Deras styrkeområde är nischmarknader och att vara disruptiva uppstickare på marknaderna med innovativa affärsmodeller. Men på grund av fragmentering har små och medelstora företag ofta svårt att skala upp sin verksamhet. För närvarande måste företag inom informations- och kommunikationsteknologisektorn (IKT) genomgå olika certifieringsprocesser för att sälja sina produkter och tjänster i hela EU. Mot denna bakgrund har EU-kommissionen inlett ett arbete med att skapa ett gemensamt ramverk för certifiering för cybersäkerhet.

EU:s Cybersecurity Act kan betraktas som ett stort steg framåt inför skapandet av en gemensam europeisk marknad för produkter och tjänster för cybersäkerhet. För första gången införs en EU-omfattande ram för certifiering av IKT-produkter, tjänster och processer. Trots att de är frivilliga, kan systemen harmoniseras mot en cybersäkerhetscertifiering i hela EU och därmed eliminera befintliga hinder för små och medelstora företag från att göra affärer över gränserna.

Vidare gör certifikaten det möjligt för kunder att bättre förstå säkerhetsfunktionerna för en produkt eller tjänst som de vill köpa, och bidrar därför till ökad marknadsöppenhet. Varje certifieringsschema kommer att specificera vilka kategorier av IKT-produkter, tjänster och processer som omfattas, och ange skräddarsydda cybersäkerhetskrav. Kraven kommer sannolikt att definieras med hänvisning till standarder eller tekniska specifikationer. Slutligen kommer ett dokument att beskriva utvärderingstyp av en produkt, tjänst eller process (till exempel självutvärdering eller utvärdering från tredje part) och den avsedda säkerhetsnivån. Exempelvis innebär en hög säkerhetsnivå att en certifierad produkt har klarat de strängaste säkerhetstesterna.

Informationssäkerhet i samhällsviktiga tjänster

EU:s NIS-direktiv ställer krav på säkerhet i nätverk och informationssystem. Reglerna omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster. Direktivet införlivas i den svenska rättsordningen genom lagen om informationssäkerhet för samhällsviktiga digitala tjänster (SFS 2018:1174) och regeringen har beslutat om en förordning (2018:1175) kopplat till den nya lagen.

Både leverantörer av samhällsviktiga tjänster och digitala tjänster ska rapportera incidenter till MSB. Det är även möjligt för frivilliga att rapportera incidenter inom ramen för NIS-regleringen.

Reglering av informationshantering hos statliga myndigheter

Informationssäkerhet i verksamheter byggs i stor utsträckning upp genom systematiskt arbete som involverar ledningen, de grundas på risk- och sårbarhetsanalyser och rätt vidtagna åtgärder. Krav på att statliga myndigheter ska se till att informationshanteringen uppfyller krav på säkerhet finns i förordning (2015:1052) om krisberedskap och höjd beredskap. Myndigheten för samhällsskydd och beredskap, MSB, föreskriver dessutom att myndigheter ska rapportera in IT-incidenter och dels införa ett ledningssystem för informationssäkerhet. I det arbetet ska standarderna ISO/IEC 27001:2014 och ISO/IEC 27002:2014 beaktas.

Lagen om elektronisk kommunikation

Lagen om elektronisk kommunikation reglerar hur information ska hanteras i elektroniska medier och vänder sig främst till telekommunikationsoperatörer. Den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster, ska se till att verksamheten uppfyller rimliga krav på god funktion och teknisk säkerhet. Detta bland annat för att säkerställa att de elektroniska kommunikationerna fungerar. Det är även viktigt att skydda uppgifterna som hanteras i de elektroniska näten. Enligt lagen ska den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst även vidta lämpliga åtgärder för att skydda behandlade uppgifter. Vilka åtgärder som vidtas beror på risken för integritetsintrång, tillgänglig teknik och kostnader.

Inom hälso- och sjukvården hanteras stora mängder ur integritetssynpunkt känslig information. Det är av stor vikt att informationshanteringen inom hälso- och sjukvården är organiserad så att den tillgodoser patientsäkerhet, god kvalitet och kostnadseffektivitet. Att säkerställa respekt för patienters och övriga registrerades integritet är prioriterat, liksom arbetet med att säkerställa att inga obehöriga får tillgång till dokumenterade personuppgifter.

Bilaga 2. Säkerhetsåtgärder – några exempel på basskydd

Det är svårt att skydda sig, och i stort sett omöjligt att skydda sig helt, men det går att vara mer förberedd. Säkerhetsåtgärder varierar från ett basskydd till avancerade strategier, taktiker och säkerhetslösningar Tekniska verktyg behövs, men den enskilt största osäkerhetsfaktorn finns i hur varje människa beter sig och använder digitala produkter och tjänster. Genom att höja medvetenheten om de vanligaste riskerna, och hur de kan motverkas, kan vi också ändra vårt beteende. Ett bra sätt är att låta testa säkerheten av en tredje part, att göra ett penetrationstest.

IT-säkerhet har olika perspektiv

IT-miljön är mer komplicerad idag än tidigare. Från stationära datorer sammankopplade i ett internt system med ett lokalt nätverk, har vi nu system, program och filer i molnet, och vi loggar in på olika typer av nätverk från olika platser. Företagets kontroll över vad som händer och vilka risker som finns, blir en allt större utmaning att hantera.

Ett företag behöver betrakta sin IT-miljö ur ett bredare perspektiv än tidigare. Det kan omfatta företagsunika system och nätverk som företaget själv har kontroll över, men vanligare är att IT-miljön kontrolleras av någon annan aktör. Det är viktigt att reflektera över var systemen finns, vilka leverantörer som anlitas och hur informationen nås. Det är också viktigt att reflektera över vem på företaget som använder vilka tjänster, när, till vad och hur det går till. Ett företagsinternt perspektiv behöver ta med personalens situation, både på och utanför arbetsplatsen.

Exempel på hur ett företag kan skapa en bassäkerhet

Syftet med denna rapport är inte att fungera som en utförlig guide för hur företag kan sätta upp sina säkerhetslösningar. Små och medelstora företag som är användare av IKT, Informations- och kommunikationsteknologi , kan skapa en bassäkerhet genom att arbeta med sexstegsmodellen nedan[11].

Inventera vilken information som är mest kritisk

Vilken information hos företaget är viktigast? Klassificera informationen och gör riskanalyser. Utgå från egna krav - produktion, kvalitet, leverantörer, varumärke m.m. Beakta externa krav från lagstiftare, samarbetspartner och leverantörer. Skapa en medvenhet om säkerhet i företaget. IT-miljön ska ges ett skydd som motsvarar behovet.

[11] Sex viktiga områden inom Säkerhet, Oscarson Security 2019, Presentation MSB.

Säkra IT-miljön

Skydda IT-miljön mot intrång och skadlig kod. Gör uppdateringar av programvara omedelbart. Använd starka lösenord och stark autentisering - använd tvåfaktorautentisering eller annan stark autentisering som BankID. Säkerhetskopiera regelbundet. Skydda mobila enheter.

Efterlev externa krav

Håll er uppdaterade på lagar, förordningar och föreskrifter, till exempel dataskyddsförordningen, GDPR. Var uppmärksam på kunders och andra intressenters krav och förväntningar.

Ställ krav på leverantörer

Ställ rätt krav på leverantörer som systemleverantörer, outsourcade IT-tjänster, molntjänster, internetoperatörer, webbplats med mera. Etablerade ramverk som är bra att använda som grund är till exempel SS-EN ISO/IEC 27002. Använd personuppgifts-biträdesavtal enligt GDPR.

Testa säkerheten

Uppdra åt en extern oberoende expertis att utföra penetrationstester. Genomför test av den egna IT-miljön och test av leverantörers säkerhet.

Säkerhetskultur och kompetens

Säkerhetsarbetet börjar på ägar- och ledningsnivå och gäller sedan alla medarbetare i organisationen. Säkerhetstänket gäller även utanför arbetsplatsen, till exempel vid resor samt uppkoppling och samtal i offentliga miljöer. Skapa vaksamhet mot exempelvis attacker via nätfiske, och andra hot och sårbarheter.

Källförteckning

A Framework for improving cybersecurity discussions within organizations, Jason Choi, McKinsey.

Att stärka allmänhetens samt små och medelstora företags motståndskraft mot it-incidenter, MSB 2018–03080.

Arbetet som aldrig tar slut, Tema: Dataskydd, Computer Sweden, mars 2020.

Building your cybersecurity roadmap, Andre Theus, Productplan.

Bra överblick och automatisering är nyckel till god it-säkerhet IDG, 2020-01-31.

Cybersecurity Attack Trends, CheckPoint Software Technologies LTD, 2019 Mid Report.

Cyber Threat Alliance (www.cyberthreatalliance.org).

Cybersecurity Considerations for IoT Product Design, IoTforall, 2019.

Cybersecurity for startups: A step-by-step guide, Forbes, 2019.

Cyber Security Posture for Competitive Advantage, Edge UK Org.

Datainspektionen slår larm: Svenskarna rasar mot Mr Koll, Breakit, 28 januari 2020.

Datorstödd utbildning för informationssäkerhet (DISA), MSB.

Dataföreningen kompetens. Säkerhetsutbildningar inom flera områden och nivåer, varav några följer standarden ISO/IEC 27000.

Digitalisering för ökad konkurrenskraft, IVA 2019.

Den smarta industrin. Nuläge, framtid och science ficition, Automation Region, 2019.

ENISA – Cyber security culture guidelines: Behavioural Aspects of Cyber Security, December 2018.

European Commission, Cybersecurity, Reciliance, Deterrence and Defence, State of the Union 2017.

Four steps to shift security to your product development lifecycle, Scott Clarke, Teachbeacon.

Global Cyber Security Market 2019-2024. Industry analysis by Growth Potent, 2019.

Here are the biggest cybercrime trends ofh 2019, World Economic Forum.

Here are the world´s top 20 cybersecurity companies, Paganresearch.

How to use cybersecurity to gain a competitive advantage, Bizcatalyst360.

Informationssäkerhet för små företag, Rekommendationer för dig som driver eget företag med upp till 10 anställda, MSB, Publikation MSB1304.

IT-säkerhets- och informationssäkerhetsutbildningar i Sverige, FOI, Amund Hunstad, Ioana Rodhe, 2015.

Kvalitetsmagasinet, Bristande kunskap hotar it-säkerheten, 17 december 2018.

Modern cybersecurity is inaccessible to smaller companies – and that's bad for you, The Next Web.

Nio typer av skadlig kod och hur du känner igen den, Techworld IDG, 2019-05-04.

Näringslivets Säkerhetsdelegation (NSD).

Ny rapport visar på växande digital klyfta mellan små och stora företag. Telias Digitala Index, Telia 2020.

Möjligheter för Sverige i digitaliseringens fotspår, Digital McKinsey, 2017.

Privacyinternational (www.privacyinternational.org).

Product manager in cyber security world, Medium, 2018.

PWC, Nordic Cyber Crime Survey, 2020.

PWC, Mapping and managing cyber risks from third parties and beyond, 2020.

RISE Cybersecurity, On-going National and International Initiatives, Shahid Rasa.

Skydda din IT-miljö, En guide till medvetet säkerhetsarbete i mindre teknikföretag, Teknikföretagen, 2019.

Security for Startups: The Affordable Ten-Step Plan for Survival in the Cyberspace, David Cowan, Bessmer Venture Partners 2015.

Selling cybersecurity and privacy: Why cybersecurity is the new competitive advantage for retaliers, Cap Gemini.

Strategic Cybersecurity, KTH Executive School, 2019.

Secure your startup: cybersecurity advice for the trenches, Coxblue.

Small Business Administration, Business guide – small business cybersecurity, USA.

Stöldskyddsföreningen.

The EU Cybersecurity Act at a Glance, European Digital SME Alliance, Position Paper, 14 january 2020.

These will be the main cyber secuity trends in 2020, World Economic Forum.

Turning cyber security into a growth driver, KPMG 2019.

Under used, Under threat, five critical technology challenges small business need to owercome now, First Voice 2019.

Verksamt.se, Skydda ditt företag.

Why cubersecutity should be taken more seriously by small and large companies alike, Thomas Ohr, november 20, 2019.

Why Third Party Risks Matters on Cybersecurity, Booz Allen Hamilton.

www.informationssäkerhet.se , MSB.