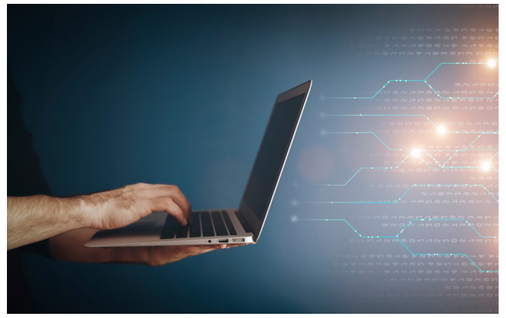
Arkiv Information Teknik

Nr 1
2023

Informationsäkerhet

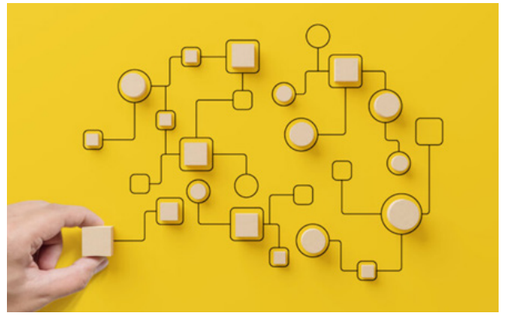
Missa inte att anmäla dig till våra kurser



Digital endagskurs
Systemvetenskap för informationshanterare

Datum: Onsdag den 18 oktober 2023.

Med utgångspunkt i ArkivIT:s erfarenhet från många arkivprojekt har vi sammanställt de centrala begrepp och metoder inom systemvetenskap som du har stor nytta av att känna till i ditt arbete som informationshanterare/arkivarie.



Digital halvdagskurs
Processbaserad arkivförteckning – Hur gör man?

Datum: Torsdag den 19 oktober 2023.

Har du försökt att förteckna arkivet processbaserat, eller verksamhetsbaserat som det också kallas, och tycker du det var knepigt? Det är du inte ensam om. Vi går igenom hur man förtecknar processbaserat/verksamhetsbaserat, vilka valmöjligheter som finns och vad som är grundläggande krav.

Endagskurs
Informationssäkerhet för arkivarier och registratorer

Datum: Torsdagen den 16 november 2023.

Både informationssäkerhetssamordnaren, arkivarien och registratorn arbetar strategiskt med informationshantering. Samtliga rollerna har mycket att vinna på att samarbeta. På denna kurs får du en orientering i hur LIS (ledningssystem för informationssäkerhet) fungerar och om vad standarderna för informationssäkerhet handlar om. Vidare så kommer vi att ta upp praktiska exempel på hur och om vad man kan samarbeta.

För mer information och anmälan:
https://arkivit.se/vara-tjanster/kurser/

Innehåll

Arkiv Information Teknik, nr 1 2023

Chefredaktör: Alexandra Meija
Redaktör/korrektur: Stina Bringsarve
Redaktör: Leif “Peppe” Pettersson
Redaktör: Lars Berglund
Redaktör: Roger Broberg
Korrektur: Anders Hedman
Korrektur: Clara Ovemyr
Formgivare: Karin Sahlander
Utgivare: ArkivIT AB

Tryck: Sibtryck
ISSN: 2003-1351

Bildmaterial:
Skribenternas egna
unsplash.com

Målet med Arkiv Information Teknik är att bjuda in till en bredare diskussion med olika perspektiv och tankar kring informationshantering utifrån dagens förutsättningar. Det finns också en ambition att skapa en diskussion som breddar bilden av vad informationshantering kan vara. Skribenterna ansvarar själva för de åsikter och de fakta som förmedlas i artiklarna. Innehållet i tidskriften speglar inte nödvändigtvis ArkivIT:s uppfattning.

Medverkande skribenter i detta nummer:

Roger Broberg
Sam Ekenkrantz
Johan Onerhed
Joakim Söderberg
Tobias Ander
Martin Palmqvist
Mats Österlund
Tom Sahlén
Andrew Tutt-Wixner
Eric Hjelmestam
Leif “Peppe” Pettersson
Daniel Lilliehöök
Mats Andréasen
Per Lagerström
Sebastian Nisser Blanck
Kent Illemann
Lars Morre Mårelius
Micke ”Lex” Lexelius
Martin Karlqvist
Jonas Hedbäck
Kim Hakkarainen
Martina Engsjö-Lindgren

Ledare

Informationssäkerhet, med all säkerhet väcker det ordet en mängd känslor och associationer hos den som stöter på begreppet. Jag misstänker att det sträcker sig från allt mellan ordning och reda, lätt panik, dåligt samvete, frustration eller rent av att det är ett fantastiskt verktyg för att skydda sin information. Informationssäkerhet, med all säkerhet väcker det ordet en mängd känslor. Vi har alla olika relation till det och där en del får skräck i blicken samt känslor av panik, ett dåligt samvete eller blir bara allmänt frustrerade. Våra skribenter har dock en annan syn och många av demassocierar begreppet till ordning och reda och tycker att det är ett fantastiskt verktyg för att skydda information.

Lätt panik var det första jag fick i mina tankar när mina kollegor Lars Berglund och Roger Broberg föreslog temat för det här numret på ArkivIT:s sommarfest 2022. Tidigare nummers teman har hela redaktionen varit förtrogna med, men det här temat, för redaktionen, kan jämföras med att segla ut på främmande vatten mitt under en rasande storm. Vi kände inte till farvattnen och vi hade ingen aning om vad vi kunde vänta oss där ute. På ArkivIT tar vi oss dock an uppgifter med stor nyfikenhet. Undertecknad har under våren läst två kurser på universitetet med inriktning informationssäkerhet för att bli mer förtrogen i ämnet, och med hjälp av våra egna informationssäkerhetsspecialister (våra fyrar) som gett förslag till artiklar och som verkat som redaktionsmedlemmar tror jag att vi till slut nått fram till land.

I det här numret kommer du att få läsa om olika aspekter av informationssäkerhet. Vi som arbetar inom arkiv känner förmodligen igen aspekterna på korrekthet, konfidentialitet och tillgänglighet, då de angränsar till vårt arbete med arkiv, d.v.s. att informationen ska vara korrekt, skyddad och tillgänglig. Som vi får läsa om har dock vi och informationssäkerhetsspecialisterna olika ingångar till informationshanteringen. Som ett försök att ena dessa finns en tanke kring att sammanlänka Säkerhets-KLASSA med Informations-KLASSA som du får möjlighet att fördjupa dig i.

ISO 27000 och MSB:s infosäkkollen samt NIS-direktivet. Vi tar även upp cybersäkerhet och informationssäkerhet vid systemutveckling. Flera av skribenterna går in på den mänskliga faktorn samt hur och varför man bör utbilda sin personal i informationssäkerhet, och de betonar även att det är viktigt att bygga en kultur kring informationssäkerhet där det blir en naturlig del av vardagen. Och i samband med det beskrivs hur man kan och bör arbeta inom organisationer för att skydda sin information och vilka verktyg som finns tillgängliga. Det rör både vad man kan göra internt, och vad man bör göra med hjälp av externa tjänster. Vi behandlar också områden som öppna data, molntjänster och Teams.

För mig kändes informationssäkerhet tidigare som något väldigt tekniskt, men som med all teknik är det alltid en människa som står bakom. Och som vi får läsa är det ofta den mänskliga faktorn som skapar luckor i arbetet med informationssäkerhet. Dessa “luckor” kan vara personer som tar fram bristfälliga kravställningar, som klickar på länkar i mejl, som lämnar sin dator en minut med tjänstekortet i ”för jag ska ju bara hämta en kaffe”. Om artiklarna har lärt mig något så är det att med kunskap kring frågorna så minskar man risken för en incident. Du som läser den här tidningen är därmed på god väg att täppa till säkerhetsluckorna!

Alexandra Meija
Chefredaktör Arkiv Information Teknik

Och som vanligt vill jag tacka min eminenta redaktion med Anders Hedman, Stina Bringsarve, Leif Pettersson och Karin Sahlander. Ett extra stort tack till gästande redaktionsmedlemmar Lars Berglund och Roger Broberg samt till Clara Ovemyr som hjälpt till med korrekturläsningen.

Alexandra Meija

Yrke: Projektledare/arkivarie/ chefredaktör för denna eminenta tidning

Arbetsplats: ArkivIT

Borta bra men ”hemma” bäst. Efter ett kort äventyr ute i arbetslivet är jag tillbaka på ArkivIT i rollen som projektledare som jag kombinerar med mina erfarenheter från arkiv och registratur. Den bästa kombinationen med andra ord!

Konsten att skydda sin information

Informationssäkerhet är en viktig del av informationshantering. Kraven på informationssäkerhet skiljer sig mellan olika typer av verksamheter. Statliga myndigheter har det som lagkrav, kommuner är inte tvingade att bedriva informationssäkerhetsarbete, men bör göra det, privata verksamheter gör det på frivillig basis. Kravet eller behovet av att skydda sin information avgör vilken nivå på informationssäkerhet organisationer bör ha.

Varför behöver vi ha informationssäkerhet? Informationssäkerhet kan ibland uppfattas som krångligt eller hämmande på kreativiteten, men den finns där för att informationen ska hanteras på ett korrekt sätt. För många är informationssäkerhet ett onödigt ont, men ett systematiskt informationssäkerhetsarbete är ett led i att identifiera vilken information som är viktigast för, oss och på så sätt kan vi identifiera vilken som är mest skyddsvärd. I en utopisk värld skulle all information vara öppen och tillgänglig för alla. Och då skulle vi inte heller ha behov av att skydda den, möjligen förhindra att den förstörs, men i övrigt skulle den vara fritt åtkomlig för alla. I vårt samhälle strävar vi mot öppenhet och transparens, som regleras i offentlighetsprincipen, men det finns även lagar och regler som begränsar åtkomsten till viss information såsom offentlighets- och sekretesslagen. I samma ögonblick som vi sätter upp hinder eller begränsningar kring den information vi har, så behöver vi införa olika skyddsmekanismer för att uppnå det tänkta skyddet. En del tror att systematiskt informationssäkerhetsarbete syftar till något slags strikt regelverk som ska införas och som alla ska följa blint och utan variation. Det är tvärtom. Informationssäkerhet innebär ett strukturerat arbetssätt för att uppnå kraven på att skydda informationen, att verksamheten får information och verktyg till vad som ska skyddas och hur. Då behovet att skydda informationen är olika beroende på vem som är intressent, behöver informationssäkerheten vara flexibel men ändå effektiv. Exempelvis så kan det på en myndighet finnas information som inte lämnas ut till allmänheten med hänvisning till sekretess. Men, beroende på vad informationen innehåller, kan det krävas att tillgången till informationen begränsas även inom myndigheten, att informationen enbart är tillgänglig för de som har behov av att komma åt den i tjänsten. Privata företag behöver inte följa lagar om offentlighet eller sekretess. Företaget vill främst skydda sin information mot sina konkurrenter. Det kan till exempel gälla framtidsplaner, uppfinningar, arbetsmetoder m.m. Information som om den inte kommer ut kan skapa ett försprång till företagets konkurrenter och därmed möjlighet för företaget att växa. Ökad digitalisering, ökad hotbild mot Sverige från främmande makt, brottslighet och enorma mängder information är några faktorer som driver på behovet av en god informationssäkerhet.

Vad är syftet med informationssäkerhet? Eftersom informationstillgångar skiljer sig, beroende på känslighet, krav på äkthet m.m., behöver vi hitta ett sätt att värdera dessa utifrån krav på eller behov av skydd. När vi pratar om krav menas i första hand lagar och regler, samt krav utifrån standarder. Men det finns så mycket annan information, bortsett den som styrs av lagar, regler och standarder, som av olika anledningar har behov av skydd.

Vem bestämmer vilket skydd sådan information ska ha? Inom informationssäkerhet har vi ett begrepp som heter informationsägare. Det kan vara en enskild person eller en organisatorisk roll, exempelvis en chef. Det är informationsägaren som ska besluta hur informationen ska skyddas och hanteras. Förr i tiden låste man bara in det man inte ville att andra skulle se i ett skåp eller en låda. I dag är det inte lika enkelt. Förutom att

mängden information i dag är ofantligt mycket större, är den inte lika fysisk som tidigare. Fortfarande finns det viss information i fysiskt format men det blir ovanligare. Utvecklingen och digitaliseringen har gjort att vi hanterar enorma mängder information utan att behöva ett enda papper. Det här ställer naturligtvis mycket större krav på en god informationssäkerhet.

”Eftersom felaktigt hanterande av information kan få stora konsekvenser för verksamheten, behöver en god informationssäkerhet införas innan något oönskat sker.”

Hur uppnår vi en god informationssäkerhet? Egentligen bara genom sunt förnuft och en gnutta konspiratoriskt tänkande. Nästan alla gör dagligen normala riskbedömningar, som valet mellan att cykla på E4:an eller cykelvägen, trots att den senare är längre. De allra flesta vet vilken information som kan spridas och vad man bör behålla för sig själv eller sina närmaste. Det här fungerar för individer, men en verksamhet behöver ha samma riskhantering och styrning för alla i verksamheten. Det behöver utformas ett regelverk och en kultur, så att alla vet vad som gäller. Om det inte finns någon internt som besitter kunskap om detta, så är det lämpligt att hyra in någon som arbetar med dessa frågor dagligen. Eftersom felaktigt hanterande av information kan få stora konsekvenser för verksamheten, behöver en god informationssäkerhet införas innan något oönskat sker. En professionell informationssäkerhetsrådgivare kan med erfarenhet och kunskap ganska snabbt etablera en grund för säkerhetsarbetet. Många i verksamheten bygger sedan vidare på denna grund, mot målet: en god informationssäkerhet. Hur ska du som informationsägare veta vad som är ett lämpligt skydd för en viss information? Sätta upp fingret i luften eller killgissa? Inom informationssäkerhet har det under lång tid utvecklats tankesätt och modeller för att kunna bedöma hur känslig en viss information är. Vi kallar det för informationssäkerhetklassificering. Det är ett sätt att gradera behovet av skydd. Utifrån denna klassificering finns en mängd olika skydd som bedömts vara lämpliga. Det låter ju enkelt. Men nu finns det en joker i leken, risk. Att sätta in alla skyddsåtgärder skulle vara opraktiskt och dyrt, men de skyddsåtgärder du väljer ska fortfarande vara effektiva. Genom att bedöma risk, kan vissa säkerhetsåtgärder uteslutas och andra finns kvar. För att vi ska kunna göra arbetet på ett systematiskt och likartat sätt, togs en internationell standard fram år 2013. Den heter Ledningssystem för informationssäkerhet. Standarden består av två huvuddelar: ISO 27001 innehåller kraven och ISO 27002 innehåller föreslagna skyddsåtgärder (riktlinjer) som kan behövas. Serien består utöver detta av ett flertal standarder för specialområden.

Eftersom standarden berör ett område med mycket snabb utveckling och förändring, behöver den revideras ibland. Den senaste revideringen är från år 2022. Digitaliseringen har vuxit explosionsartat med nya tekniker, molntjänster av olika slag m.m. Allt detta har lett till att behovet av informationssäkerhet är större nu än tidigare. Den reviderade versionen av ISO 27000 utgår mer i vad skyddet ska vara till för och mindre kring specifika tekniska detaljer. Exempelvis har ordet ”nätverk” ersatts med ”informationsöverföring”. På så sätt inbegriper standarden fler tekniska lösningar, än just den tekniska termen nätverk. Om du skickar information från din telefon, så tänker du knappast att du arbetar i ett nätverk, utan du ser det som att du gör en informationsöverföring. Ett annat begrepp som introducerats i den nya versionen är ”livscykelhantering”. Med det menas att det ska finnas en dokumenterad plan från det att behovet identifierats tills systemet avvecklas. Från det att behovet finns för att införa exempelvis ett nytt IT-system, ska hela systemets livscykel börja dokumenteras med uppgifter om ansvariga, förvaltning, beräknad livslängd på komponenter och information, avställningsplan m.m. Just det här med att avveckla ett system är väldigt olika mellan ett privat företag och en myndighet. Ett privat företag kastar bara ut sitt gamla system och installerar ett nytt. En myndighet måste kontrollera vad som ska bevaras och vad som kan gallras bort. Tyvärr är en vanlig åtgärd hos myndigheter att bara ”parkera” det gamla systemet och hoppas på det bästa rörande framtida åtkomst till informationen. D.v.s. att man bara rycker ut sladden ur väggen, utan att avistallera det. Det innebär en informationssäkerhetsrisk samtidigt som det utgör en skuld till dem som i framtiden behöver ta sig an avställningen, samtidigt som det finns en risk att man inte uppfyller arkivlagens krav på bevarande av allmän handling. I den reviderade versionen har antalet säkerhetsåtgärder minskat från 114 till 96. Inga åtgärder har tagits bort men några likartade har slagits ihop och därtill har det tillkommit 8 nya åtgärder. I den nya versionen finns bättre förklaringar och tydligare exempel för att det bättre ska belysa om åtgärden är tillämpningsbar eller inte. Det har även införts något som kallas attribut, detta är en slags märkning av säkerhetsåtgärderna för sortering och underlättad återsökning.

Sammanfattningsvis kan man säga att den reviderade standarden har ett mer holistiskt perspektiv, och den försöker att inte låsa in sig i detaljerade tekniska lösningar. Man bör samtidigt komma ihåg att standarden är internationell och har kompromissats fram. Det gör att vissa delar kan vara mindre förekommande i Sverige samt att vi i vissa delar har lagregleringar som inte finns i andra länder.

Det finns inget motsatsförhållande mellan informationssäkerhet och bevarande av information. Informationssäkerheten sätter upp regler för informationen. Det kan gälla behörigheter, var det får lagras och vilka system som är tillåtna. Om informationen ska bevaras, behöver den kanske ”datummärkas” beträffande hur länge nuvarande klassning gäller. Det som är superkänsligt i dag, kanske är sökbart på webben om några år – eller inte. Arkiv, registratur och informationssäkerhet har många beröringspunkter gällande informationshantering. Med ett bra samarbete kan positiva effekter uppstå vilket gynnar alla.

Den här artikeln fokuserar på behovet av informationssäkerhet och att etablerade modeller och standarder finns på plats. Jag vill dock understryka att det krävs erfarenhet och kunskap för att kunna omsätta detta i verksamheten. Om det görs på fel sätt blir det ett regelverk utan verkan.

Roger Broberg

Roll och arbetsplats: Arbetar på ArkivIT med dataskydd. Främst som dataskyddsombud, men med stor vikt på informationssäkerhet.

Utöver lång erfarenhet inom IT i olika roller driver jag även utbildningar och seminarier inom dataskydd. Jag har verkat som dataskyddsombud (DSO) på ett stort antal organisationer. I denna artikel vill jag ge min syn på hur man kan tänka kring det professionella dataskyddsarbetet.

Metoder för ett effektivare informationssäkerhetsarbete

Hur kan man med stöd av mätning bedriva ett systematiskt riskbaserat informationssäkerhetsarbete? Och hur kan man effektivt arbeta medmedarbetarnas medvetenhet i frågan

Information är en av de värdefullaste och känsligaste tillgångarna i de flesta verksamheter. Utan att kunna lita på att man har tillgång till informationen eller att den är rätt och riktig så får alla verksamheter mycket stora problem. Det gäller oavsett om det handlar om bokföring, löneinformation, kundinformation etc. Därför blir allt fler ledningsgrupper medvetna om vikten av att skydda verksamhetens känsliga information. De kan även ha ökade krav från kunder och myndigheter samt en ökad hotbild mot verksamheten.

Arbetet med att skydda informationen – informationssäkerhet – är ett stort område i alla organisationer men tvingas ofta arbeta med begränsade resurser. Det leder i regel till utmanande frågor som:

Vilken information har vi och vilket värde har den för verksamheten?
Var hanteras och lagras den?
Vilka lagkrav gäller för den?
Vilka risker är den utsatt för?

Trots begränsade resurser är det viktigt att få till ett kvalitativt systematiskt informationssäkerhetsarbete, något som blir en allt större utmaning. Detta arbete måste följas upp efter hand både vad gäller medvetenheten hos medarbetarna och kvaliteten på införda säkerhetsåtgärder som syftar till att skydda informationen

Att arbeta med riskhantering för att skydda sin information
Det är viktigt för alla organisationer att säkerställa att informationen hanteras på ett säkert sätt. Däri ligger att se till att den är skyddad med relevanta skyddsåtgärder för att minimera risken för dataintrång och andra säkerhetsproblem. Att ta stöd i ISO/

”I många undersökningar pekas vi medarbetare ut som den kanske största informationssäkerhetsrisken. Som tur är blir medarbetarna alltmer medvetna om säkerhetsfrågor.”

IEC 27000-standarderna kan vara en bra idé. I dem kan man få stöd i att utveckla och implementera ett systematiskt riskbaserat informationssäkerhetsarbete. Man brukar benämna det som ett ledningssystem för informationssäkerhet (LIS). LIS är en strukturerad och systematisk metod för att hantera och skydda sina informationstillgångar genom att identifiera, bedöma och hantera risker. Ett sätt att arbeta med frågan är att ta fram en riskhanteringsplan som inkluderar följande steg:

1. Identifiera informationstillgångar – Organisationen identifierar och värderar alla informationstillgångar som behöver skyddas, till exempel kundregister, anställningsregister, känsliga avtal, e-postmeddelanden, databaser med mera.

2. Bedöm hot och sårbarheter – Organisationen bedömer vilka hot som kan påverka informationstillgångarna, till exempel dataintrång, virus, sabotage eller naturkatastrofer, samt bedömer sårbarheter i systemen som kan utnyttjas av hoten, till exempel bristande säkerhetskopiering, bristande autentisering eller utdaterade programvaror.

3. Identifiera risker (riskanalysprocessen) – Organisationen genomför en riskanalys av ett avgränsat område (tjänst, system, enhet) genom att identifiera vilka risker som finns.

4. Värdera risker (riskanalysprocessen) – Nästa steg i riskanalysprocessen är att värdera riskerna. För att så system-

atiskt och konsekvent som möjlig genomföra värderingen är det till stor nytta att ta hjälp av en så kallad normskala. En normskala beskriver en stegvis konsekvens som är trolig för organisationen för exempelvis områden som varumärke, pengar, person o.s.v. om risken inträffar. Och på samma sätt kan man även ha med en skala för bedömning av sannolikhet. Genom att sätta siffor på de olika alternativen (nivåerna) i konsekvensskalan kan man ha hjälp av en matematisk formel och en riskmatris för att få en övergripande bild av riskläget.

5.Planera och genomföra åtgärder (riskanalysprocessen) – Organisationen hanterar riskerna genom att acceptera risken eller välja lämpliga skyddsåtgärder för att mildra, undvika eller överföra riskerna. Det kan till exempel vara aktiviteter som utbildning, uppgradering av brandväggar, antivirusprogram, säkerhetskopiering och autentiseringsmekanismer etc. Det är bra, och egentligen nödvändigt, att alla aktiviteter får en ansvarig och ett slutdatum.

6.Följa upp och granska (riskanalysprocessen) - Organisationen följer upp och granskar sina genomförda säkerhetsåtgärder regelbundet för att säkerställa att de är effektiva och uppdaterade, förslagsvis genom mätning. Mer om mätning längre fram.

En viktig effekt av en riskanalysprocess är den medvetenhet som uppstår hos deltagarna och andra som får ta del av resultatet.

Uppdatera “den mänskliga brandväggen”
I många undersökningar pekas vi medarbetare ut som den kanske största informationssäkerhetsrisken. Som tur är blir medarbetarna alltmer medvetna om säkerhetsfrågor. Men om man inte inkluderar medarbetarna i säkerhetsarbetet kvarstår risken att vi som individer omedvetet gör ett misstag som på ett ögonblick kringgår alla tekniska och fysiska skyddsåtgärder. Samtidigt som informationssäkerheten oftast inte är en del av kärnverksamheten och därmed ibland glöms bort. Med andra ord behöver även den ”den mänskliga brandväggen” uppdateras regelbundet. Därför är det av mycket stor vikt att man planerar utbildnings- och informationsinsatser på ett sätt som ger så stor effekt som möjligt. En metod kan vara att dela upp informationssäkerhetsutbildningens innehåll i mindre block som för deltagarna är lätt att smälta och genomföra dessa block med regelbundenhet, exempelvis under vecko- eller månadsmöten. Blocken kan med fördel innehålla både en kunskapsdel och en omvärldsinformationsdel. Tanken är att arbetet med informationssäkerheten ska bli lika naturligt som att låsa dörren när man går hemifrån. Man kan också enkelt hitta händelser om informationssäkerhet att ta med som ett komplement till det interna materialet, exempelvis nyheter om incidenter eller dagsaktuella cyberhot.

Exempel på systematiskt riskbaserat informationssäkerhetsarbetet med stöd av mätning
Vad svarar man om ledningsgruppen eller någon annan del av verksamheten ställer frågan ”Hur bra säkerhet har vi” eller ”Är vi tillräckligt säkra”? Dessa är vanliga reflektioner från exempelvis en ledningsgrupp. Och frågorna är relevant då säkerheten blir allt viktigare för alla verksamheter. Då är det bra om man kan åskådliggöra säkerhetsnivån på ett lättförståeligt och trovärdigt sätt för dem. En bland flera viktiga frågor blir då hur man på ett så objektivt sätt som möjligt ”tagit reda på” vilken säkerhetsnivå verksamheten har.
En metod är att arbeta med mätning av implementerade säkerhetsåtgärder som helst täcker in både människa, organisation och teknik. Då är det till stor nytta om mätprogrammet som används går ut på att mäta prestandan (nivån) i verksamhetens säkerhetsåtgärder. Med andra ord: hur väl man har lyckats med införandet av sina säkerhetsåtgärder. Det innebär att mätprogrammet enligt vår erfarenhet bör vara utformat med ett antal fördefinierade mätpunkter där varje enskild mätpunkt följer en nummersatt kravbeskriven skala, gärna med en gemensam normnivå för varje enskild mätpunkt. Exempelvis att varje mätpunkt har en skala från 0 till 5 och att 3 är godkänd nivå (normen). Det är också bra för trovärdigheten om man kan koppla varje mätpunkt till en eller flera säkerhetsreferenser. Som bas kan man med fördel använda sig av informationssäkerhetsstandarden ISO/IEC 27001/27002, men det finns även andra lämpliga referensverk beroende på vad som ska mätas. Handlar det exempelvis om datorhallarna kan man även inkludera mätpunkter som använder sig av rekommendationer som arbetas fram av Myndigheten för samhällsskydd och beredskap (MSB). Inom ISO/IEC 27000-standarden finns även ISO/IEC 27004 som beskriver uppföljning genom bland annat mätning. Om sedan rapporten från en mätning även innehåller kommentarer och rekommendationer för varje mätpunkt som inte når upp till normnivån underlättar detta väldigt mycket det fortsatta praktiska säkerhetsarbetet. Exempelvis kan resultatet från en mätning sedan användas i riskanalysprocessen. En av de stora vinsterna med detta är att ett mätprogram täcker ett mycket större område än vad man oftast hinner med i traditionellt säkerhetsarbete. Beroende på utformning och omfattning får man en detaljerad bild av de olika delarna av informationssäkerhetsområdet, som organisatorisk säkerhet, fysisk säkerhet och systemsäkerhet.

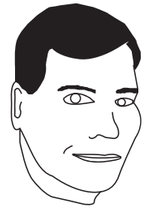
Sammanfattningsvis får man genom mätning:
• Ett tydligt och kvalitativt underlag för kommunikation med ledningsgruppen och verksamheten
• Ett bra stöd för att avgöra vilka områden som man bör genomföra riskanalyser på
• Med ett fördefinierat mätprogram kan man följa upp och jämföra den egna verksamheten över tiden

Sam Ekenkrantz

Roll: Sitechef och produktägare
Arbetsplats: Coor, Arkinet

Sam har arbetat med e-arkiv sedan 1998 och informationssäkerhet har utgjort ett ständigt centralt arbete i roller som systemarkitekt och produktägare. Intressanta utmaningarna är att få kartlägga det komplexa. Fritiden tillbringas med familjen ute i naturen eller hemma i trädgården bland odlingar och hönor.

Johan Onerhed



Roller/områden: Affärsutveckling och informationssäkerhet
Företag: Coor, Arkinet

Johan har arbetat med digitalisering och e-arkivsfrågor sedan 1995, samt 15 år med informationssäkerhet och GDPR som konsult och i olika roller.
Bästa utmaningen är att få informationssäkerhetsarbetet att fungera i verkligheten i verksamheten. Fritiden går åt till familj, vänner och motion.

Rätten till rättelse och allmänna handlingar

Att uppgifter som finns i arkiv inte ska ändras är inte så konstigt egentligen. Arkivet är ett minne över vad myndigheter har gjort, det som är bra, det som är dåligt och det som är fel. Att ändra i ett arkiv är att skriva om historia, något som jag personligen tycker att vi ska vara lite försiktiga med. Men innan uppgifterna blivit arkiverade så ska de gå att rätta. Hur detta går till eller inte går till idag är det den här artikeln kommer att kort belysa.

Principen om korrekthet är en grundläggande princip inom informationssäkerhet och dataskydd. Uppgifter ska vara korrekta helt enkelt. I dataskyddsförordningen (GDPR) översätts denna princip till rätten till rättelse. En rättighet utan undantag, förutom såklart i de fallen där lagen inte gäller. Ett sådant fall kan vara när uppgifter ska arkiveras. GDPR har nämligen en undantagsregel vad gäller just personuppgifter som ingår i arkiv, som innebär att vissa rättigheter i GDPR kan lagstiftas bort. I Sverige har rätten till rättelse för uppgifter som finns hos arkivmyndigheter lagstiftats bort genom arkivförordningen.[1]

Utmaningen kring uppgifters korrekthet
Ett exempel för att måla upp vår scen:
En man går till läkaren och klagar på att han har svårt att äta. Läkaren tittar på mannen och ser att han är olycklig, ställer frågor om mannens liv och får olyckan bekräftad. Mannens fru har precis lämnat honom, hans hund har dött och han fick nyligen sparken. Läkaren diagnosticerar mannen med depression och ätstörning. Uppgifterna förs in i mannens journal. Han får tid hos en psykolog.

Mannen går därefter till en annan läkare eftersom samtalen med psykologen inte lett till att han har fått det lättare att äta, även om han i viss mån känner sig stärkt av samtalen. Läkare 2 frågar mannen om han gillar att äta rå kyckling, till vilket mannen svarar jakande. Läkare 2 konstaterar magtarmbakterier och skriver ut antibiotika, samt föreslår för mannen att han ska tillaga sin kyckling i framtiden. Uppgifterna förs in i mannens journal. Mannen blir bättre av antibiotikan och när han lärt sig hur spisen fungerar så försvinner problemen helt.

Nu har mannen två diagnoser skrivna i sin journal som kan påverka mannens förmåga att inta föda: ätstörning samt campylobacter. Men vilken av dessa uppgifter är korrekt? Det vi vet är att mannen kan äta efter samtal med psykolog samt efter att han slutat äta rå kyckling. Vi vet också att problemen att äta inte gick över efter enbart samtal med psykolog. Detta talar för att campylobacter var rätt diagnos. Om situationen hade varit omvänd så hade däremot diagnosen "ätstörning" sett mer korrekt ut. Om en åtgärd eller två var nödvändiga för att bota mannen vet vi inte.

Allmänna handlingar
När uppgifterna förts in i mannens journal har de blivit del av en allmän handling hos myndigheten som för mannens journal, troligen regionen där mannen bor. När uppgifterna vid något tillfälle skickas till en annan myndighet blir de del av allmänna handlingar hos den mottagande myndigheten. Det finns nu uppgifter i dessa handlingar som kan vara inkorrekta, om så är fallet borde dessa uppgifter rättas. Kruxet som uppkommer är att uppgifter i allmänna handlingar inte får raderas.[2] Eller som JO skriver: *"Till begreppet allmän handling är kopplat viktiga rättsverkningar, som avser allmänhetens insyn och kontroll av myndigheternas verksamhet. En sådan handling kan därför inte utan vidare ändras. Självfallet får och skall en felaktig uppgift rättas. En felaktig uppgift får dock inte raderas bort."*[3]

Syftet med att bibehålla integriteten hos felaktiga uppgifter i allmänna handlingar är alltså för att vi som medborgare ska få en möjlighet att granska makten. En myndighet ska inte få ändra i handlingar för att det passar dem, eller för att förhindra att information sprids. Att en felaktig diagnos har ställts skall finnas kvar, annars kan myndigheten inte lära sig av sina misstag.

Men syftet med rätten till rättelse i GDPR är att värna den enskilde och principen om uppgifters korrekthet. Korrekta uppgifter leder till korrekta beslut. Inkorrekta uppgifter leder inte till korrekta beslut. Mannen ska därmed ha möjlighet att påpeka att han aldrig haft en ätstörning, om han nu inte hade en ätstörning, och få uppgiften ändrad.

Error carried forward
När jag läste matematik i gymnasiet så vägde våra uträkningar tyngre vid betygsättningen än de svar vi kom fram till. Om det blivit ett fel tidigare i uträkningen och det felet följde med fick vi avdrag för felet som var gjort men inte för att vi svarade fel, eftersom vi svarade rätt baserat på den uträkning vi hade gjort. ”Error carried forward” kallade matteläraren det här.

När en myndighet fattar beslut så gör den det på den information som kommer fram i underlaget som ligger till grund för beslutet. Om det finns felaktigheter i underlaget så följer dessa med. Beslutet blir korrekt, underlaget är fel, error carried forward. En läkare ordinerar psykolog. I vissa fall kan det här innebära att en person får ett beslut som går den emot. Den som vill överklaga ett sådant beslut kämpar typiskt sett i motvind. Beslutet är korrekt under de förutsättningar som det uppstått.

För att grunderna för ett beslut ska bli korrekta behöver uppgifterna rättas. Men detta är inte alltid möjligt. Exempelvis beskriver Försäkringskassans i sin riktlinje kring registervård situationen såhär: *"[R]ättelse inte ska ske enbart därför att uppgifter som framstod som riktiga eller rimliga när de samlades in senare har visat sig vara oriktiga."*[4] Rättelse ska alltså enligt Försäkringskassans egen vägledning inte göras om den som samlade in uppgifterna trodde de stämde överens med verkligheten när de samlades in. Försäkringskassan hänvisar även till ett

avgörande från JK och tolkar det såhär: *”För att det ska anses utgöra en felaktig personuppgift krävs att det rör sig om ett rent handhavandefel i samband med registreringen.”*[5]

Konsekvensen av det här är att vi har en myndighet, och säkert flera, som menar att uppgifter som inte stämmer överens med verkligheten är korrekta, utom om det rör sig om “rena handhavandefel” så som till exempel att ett namn stavas fel. Eftersom mannens namn stavats ”mannen” varje gång finns här inga problem.

En felaktig uppgift från en myndighet eller annan källa kommer till Försäkringskassan och kan därefter inte rättas. Uppgifterna ligger sen till grund för beslut. Mannen ges en möjlighet att påpeka det här inför beslut genom följande standardskrivelse från FK: *”Hör av dig om något i underlaget inte stämmer, eller om du vill lägga till något. Om du skickar ett brev så skriv ditt personnummer på det som du skickar in. Sista dagen för att svara är [datum om tre veckor]. Sedan kommer Försäkringskassan att fatta ett beslut.”*

Men eftersom även de uppgifter som inkommit tidigare anses vara korrekta så uppstår en situation där myndigheten trots invändningar om bristen på korrekthet i underlaget ej anser sig själv ha en skyldighet att ändra i förslaget till beslut. Mannen påpekar att han inte har en ätstörning och får följande svar: ”Försäkringskassan har gått igenom ditt ärende på nytt, samt beaktat dina synpunkter, men finner inte skäl för att ändra beslutet.”

Vem äger korrektheten?
Det intressanta i Försäkringskassans bedömning och läsning av JK:s avgörande är att JK aldrig sagt att rättelse inte är aktuellt i andra situationer än vid rena handhavandefel. Det JK konstaterade i sitt avgörande var att handhavandefel leder till ”registerskada” Men att andra fel ska bedömas utifrån allmän skadeståndsrätt.[6]

JK tog alltså aldrig upp frågan om andra felaktigheter skall rättas eller inte. Det enda de konstaterade var att felregistreringar leder till skadestånd under PUL direkt. Rätten till rättelse aktualiserades inte alls.

Vad JO konstaterat gällande rättelse är att följande kan göras för att rätta en felaktig uppgift i handlingar: *”En korrekt hantering [---] hade varit att rätta de felaktiga uppgifterna, t.ex. genom att vid respektive post ange i en tillagd, daterad och signerad rättelsemening att posten var felaktigt införd. Nämnden bör således se till att det i dess datasystem läggs in rutiner som möjliggör att felaktiga uppgifter i diariet rättas i stället för att raderas.”* [7]

Att notera i JO:s uttalande är att det i förevarande fall rörde sig om just handhavandefel, i det här fallet felaktigt införda händelser i en postlista. Någon direkt slutsats om huruvida rätten till rättelse även gäller sådant som inte är handhavandefel kan vi därför inte dra där. I stället vänder vi oss utåt, och tittar på EU.

I avgörandet av det tyska fallet HBDI-62334 noterades det att ändring av felaktiga personuppgifter, som den registrerade själv uppgett medvetet, omfattades av rätten till rättelse.[8] Därav kan vi dra slutsatsen att en källa till uppgifter i viss mån styr uppgifternas korrekthet hos mottagaren. Uppgifter som en myndighet tagit in från andra skall alltså läsas på så vis att senare uppgifter som är i konflikt med tidigare har företräde gentemot de tidigare uppgifterna. Eventuell konflikt mellan mannens diagnoser leder till att den senare är ”rätt”.

Men om både de felaktiga uppgifterna och de uppgifter som är korrekta finns med i ett beslutsunderlag så läggs en stor börda på den enskilde handläggaren att identifiera både konflikt i uppgifter samt när uppgifterna upprättades i relation till varandra. Vilken tur då att Försäkringskassan struntar i om uppgifter faktiskt stämmer överens med verkligheten eller inte i bedömningen av om de är korrekta. Då blir belastningen på handläggaren att göra en avvägning vilka uppgifter som kan ligga till grund för beslut lite enklare, eftersom alla uppgifter då kan ligga till grund för beslut. Men rätten till rättelse, den syns inte riktigt till.

Slutsats
I princip skall felaktiga uppgifter hos myndigheter rättas. Det enda undantaget till den här regeln är när handlingarna där uppgifterna finns har arkiverats. Problematiken som finns idag avseende denna rättighet är att de mer mjuka uppgifterna, så som bedömningar av olika slag, enligt vissa myndigheter inte omfattas av rättigheten. Konsekvensen blir att motstridiga uppgifter, trots att källan är densamma, båda är korrekta och kan ligga till grund för beslut. Vad det faktiska beslutet blir spelar mindre roll. Error carried forward innebär i det här fallet att mannen har en ätstörning, oavsett om han vill eller ej .

Källor:

1. Det här har lett till en viss förvirring hos hela Sveriges arkivariekår, som av någon anledning menar att arkivlagen går före GDPR men så funkar det alltså inte riktigt (mer om det i en annan artikel).

2. Mannen kan begära journalförstöring, för att få sina uppgifter borttagna från journalen. Men det här är en särskilt reglerad och lite komplex fråga i vilken det finns en stark presumtion för att uppgifterna är korrekta. JFR: Patientdatalagen 8:4.

3. JO:s ämbetsberättelse 1993/94 s. 305 – med hänvisning till konstitutionsutskottets betänkande 1982/83:12 s. 22, SOU 1984:73 s. 171 och JO:s beslut den 26 januari 1985 dnr 1131-198

4. Registervård (rättelse av personuppgifter) Dnr 9715-2018

5. JK beslut 2009-09-28, dnr 2617-08-42 - https://www.jk.se/beslut-och-yttranden/2009/09/2617-08-42/

6. ”Frågan om vad som ska anses utgöra en registerskada i PUL:s mening är inte helt lätt att besvara. I Justitiekanslerns praxis har man brukat fästa avgörande vikt vid om det är ett rent handhavandefel i samband med registreringen, eller om det också rör sig om något tankefel eller en bearbetning av uppgifterna av intellektuellt slag. I det senare fallet anses det inte föreligga en registerskada, utan då får felet bedömas uteslutande enligt skadeståndslagens regler.””

7. JO dnr 4639-2007

8. https://gdprhub.eu/index.php?title=HBDI_(Hesse)_-_62334_(IMI_Case)

Joakim Söderberg

Roll: Dataskyddsjurist

Joakim är en dataskyddsjurist som jobbat och jobbar brett med GDPR. Bland annat har Joakim varit myndighetschef på Datainspektionen på Åland, samt drivit framgångsrika processer angående enskildas rättigheter i domstol. Just nu är han dataskyddsombud i Uppsala Stift, delägare i företaget GDPR-Buddy, cirkelledare i Dataföreningen Sverige och en sporadisk bloggare på https://www.datajurist.se/

Trygg informationshantering

God informationssäkerhet handlar inte bara om att skydda verksamhetens tillgångar med hjälp av teknik. Det handlar lika mycket om att utveckla rutiner, processer och medarbetare. Många organisationer kan väsentligt öka effektiviteten i informationssäkerhetsarbetet genom att förändra kulturen.

Vi ser idag en digitalisering och ett användande av IT i situationer som var otänkbara för 10–20 år sedan. Det blir allt lättare att koppla upp sig mot internet, att sammanföra företag, organisationer, individer och saker. Digitaliseringen och utbredningen av IoT (Internet of things) sker i en rasande fart och åstadkommer enorma förändringar i samhället, såväl för oss som privatpersoner som för våra organisationer. Denna utveckling erbjuder nya funktioner och lösningar som hjälper oss att bli snabbare, effektivare och att hitta helt nya verksamhetsområden. De här förändringarna har dock en baksida om de inte genomförs på ett bra sätt.[1]

Hur gör vi då för att skydda informationen i en ny digital tidsålder där vi kopplar upp glödlampor, kylskåp, tv, hem- och företagsdatorer samt mobiltelefoner? Att låta någon bekant eller obekant låna vårt wifi när de är på besök i våra hem är lika naturligt som att låna ut toaletten. Vad kan hända, varför ska jag bry mig? Förutom nya möjligheter innebär den här utvecklingen nya risker både för våra organisationer och våra hem. Vi kan inte lägga över ansvaret på någon annan och lita på att våra tekniska prylar ger oss all den säkerhet som behövs för att vi ska känna oss säkra.

I och med den snabba förändringen i vår omvärld och vårt massivt ökade beroende av digitalisering och information – speciellt i våra organisationer – behöver även informationssäkerhetsarbetet ta flera steg framåt. Det räcker inte att enbart skydda organisationen med hjälp av teknik, policy och utbildning. Vi behöver bygga en organisation där alla förstår att de är en del av skyddet av verksamhetens information och kan vara med och bidra. En organisation där den allmänna förväntan är att varje medarbetare bidrar till informationssäkerheten, där varje medarbetare vill göra rätt, bete sig på ett informationssäkert sätt och ha rätt attityd. En organisation där det är lätt för medarbetarna att göra rätt. Det åstadkommer vi genom att skapa en informationssäkerhetskultur som stödjer verksamheten på verksamhetens och medarbetarnas villkor.

Informationssäkerhet är de åtgärder som vidtas för att hindra att information läcker ut, förvanskas eller förstörs och för att informationen ska vara tillgänglig när den behövs.[2] Detta är den gängse definitionen av vad ett informationssäkerhetsarbete innebär. Det blir dock ofta för krångligt för en verksamhet att förstå och hålla reda på olika termer inom området. En enklare definition kan vara säker informationshantering. Men oavsett hur man definierar arbetet förutsätter båda dessa definitioner underförstått att informationen eller informationshanteringen kan vara 100 procent säker. Det rimmar dock illa med de incidenter vi idag känner till. Utifrån dessa händelser blir det tydligt att vi aldrig kan uppnå 100 procent säkerhet och att informationen till exempel aldrig kommer vara tillgänglig hela tiden.

Det är egentligen bättre att prata om trygg informationshantering , då det är det vi oftast strävar efter. Informationssäkerhetsarbetet handlar i de flesta fall om att den som äger informationen ska känna sig trygg i hur den hanteras, oavsett om det rör sig om mina privata personuppgifter, organisationens egen information eller information som hanteras på uppdrag av någon annan.

Det handlar om att jag som informationsägare ska känna mig så trygg att jag kan bygga en verksamhet utifrån hur information hanteras. Men också om att jag som privatperson ska kunna lita på att en organisation hanterar mina personuppgifter på ett säkert sätt.

Dagens Informationssäkerhetsansvarig (CISO) är inte en tekniknörd som kan det mesta om it eller it-säkerhet i organisationen. Det är en person som jobbar nära verksamheten, som leder och samordnar den i arbetet med att uppnå ett adekvat skydd. Han eller hon ser över hur man förändrar sina rutiner och sin styrning och får sina medarbetare att tillämpa en säker hantering av informationen. CISO:n behöver vara en förändringsledare med uppgift att bygga en informationssäkerhetskultur i organisationen, där varje individ är en viktig del av arbetet.

Vi behöver ge medarbetarna en sund informationssäkerhetskultur att verka i, en kultur som jobbar med medarbetarnas attityder och beteendekontroll samt organisationens normer så att vi kan införa en rättvis, rapporterande och lärande miljö. Genom att göra det får vi en organisation som klarar av förändringar, incidenter och större tillbud. En verksamhet som är betydligt bättre rustad för kända och okända hot, nu och i framtiden.

CISO-rollens huvudsakliga arbetsuppgifter: leda och samordna säkerhetsarbetet
Den som är CISO har det övergripande ansvaret att leda och samordna arbetet med informationssäkerhet i en organisation. Huvudansvaret för själva informationssäkerheten följer verksamhetsansvaret, och ligger därmed inte på rollen som CISO. Källa: https://www.informationssakerhet.se/metodstodet/utforma/ 2023-07-11

Källor:

1. Mikko Hypponen.If It's Smart, It's Vulnerable (2022)

2. https://sv.wikipedia.org/wiki/Informationss%C3%A4kerhet, 2023-07-10

Tobias Ander

Har lång och gedigen erfarenhet från arbetet med informationssäkerhet i offentlig verksamhet, som CISO på Transportstyrelsen och är idag bland annat CISO på Örebro kommun.

Tobias arbetar idag aktivt med frågor kring ledning och styrning samt informationssäkerhetskultur och genomför utbildningar och föreläsningar utifrån sitt engagemang i företaget Securebyme.

Tobias vann år 2017 priset ”Årets GRC-profil” för sitt kunnande och engagemang inom governance risk compliance (god förvaltningssed, riskhantering och kravenlighet). Han är aktuell med handboken ”Informationssäkerhetskultur”.

Handboken om informations-säkerhetskultur

är en bok kantad med handfasta tips och råd, samt relevanta checklistor som hjälper dig att bygga en säkrare organisation i en digital tidsålder. Handboken tar upp det viktigaste du behöver känna till och lära dig för att utveckla och etablera en god informationssäkerhetskultur i din organisation. Handboken vänder sig även till dig som har upptäckt att det arbete ni gör idag, inte räcker för att skydda er information trots att ni följer befintliga föreskrifter, best practice och standarder.

SECURE BY ME AB
Hjälper dig att bygga
robust informationssäkerhet
securebyme.se

NIS-direktivet: informationssäkerhet för samhällsviktiga och digitala tjänster

2018 hände något historiskt. Det första NIS-direktivet började gälla i EU:s medlemsländer. Så här fem år senare har mycket förändrats i vår omvärld – covid-19-pandemin, förändrad geopolitisk situation, krig i Europa, uppmärksammade IT-incidenter – samtidigt som samhällets digitalisering bara fortsatt. Med bakgrund i den ökade hotbilden och det förändrade omvärldsläget har nu NIS2-direktivet antagits och börjar gälla hösten 2024.

Det första NIS-direktivet (The Directive on security of network and information systems) var den första EU-regleringen med syftet att höja informations- och cybersäkerheten i unionen. Bakgrunden till direktivet är den roll som nätverks- och informationssystem har kommit att spela som möjliggörare för såväl ekonomin som för andra viktiga samhällsfunktioner. Beroendet av dessa system gör att incidenter som inträffar i dem riskerar att orsaka allvarliga konsekvenser för unionen. Regleringen riktar sig därför mot de som tillhandahåller tjänster som är viktiga för samhället och ekonomin – så kallade leverantörer av samhällsviktiga och digitala tjänster (NIS-leverantörer).

De samhällsviktiga tjänsterna delas in i sju sektorer:

•Bankverksamhet

•Digital infrastruktur

•Energi

•Finansmarknadsinfrastruktur

•Hälso- och sjukvård

•Leverans och distribution av dricksvatten

•Transport

”På så sätt kommer NIS2 att få betydligt vidare påverkan än enbart på de sektorer som explicit anges i direktivet.”

För att minska sårbarheterna ställer direktivet krav på en miniminivå av säkerhet i nätverks- och informationssystem. Förutom att höja den generella säkerhetsnivån bidrar direktivets krav även till att likrikta säkerhetsåtgärderna inom unionen. På grund av att det är ett direktiv och inte en förordning så är det dock upp till varje medlemsstat att implementera direktivet i nationell lagstiftning vilket leder till att vissa mindre skillnader kan förekomma mellan medlemsländerna. I Sverige implementerades direktivet genom lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

I denna framgår krav på:

•Systematiskt och riskbaserat informationssäkerhetsarbete

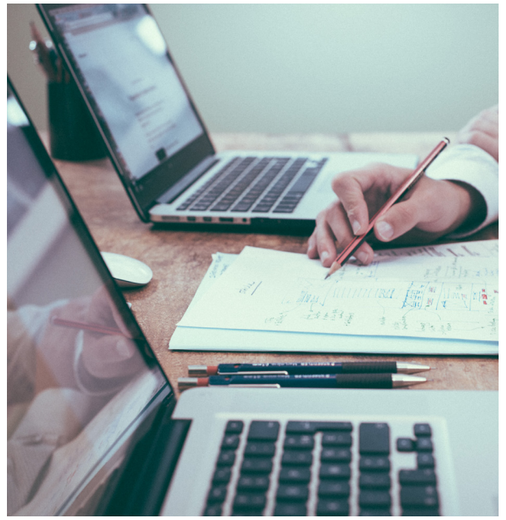
•Riskanalys med åtgärdsplan

•Tekniska och organisatoriska åtgärder för att hantera risker

•Förebygga och minimera konsekvenser av incidenter

Fler detaljer kring dessa krav ges i förordning (2018:1175) där även Myndigheten för samhällsskydd och beredskap (MSB) och ett antal tillsynsmyndigheter ges mandat att genom föreskrifter specificera kraven ytterligare.

Även om efterlevnad av kraven och ett välutformat förebyggande arbete minskar riskerna är det dock svårt att helt kunna skydda sig mot IT-incidenter. Detta hanteras inom NIS genom



obligatorisk incidentrapportering av de incidenter som påverkar tillhandahållandet av den samhällsviktiga eller digitala tjänsten. I Sverige innebär kraven på incidentrapportering att NIS-leverantörer ska rapportera de incidenter som orsakar störningar som har betydande inverkan på kontinuiteten i den tjänst man levererar. En första rapport ska ske senast sex timmar från att incidenten identifierats som rapporteringspliktig och sedan i två ytterligare skeden efter 24 timmar respektive fyra veckor allt eftersom incidenten hanteras och mer information framträder.

Förutom kraven på säkerhetsåtgärder och incidentrapportering för verksamheter innehåller NIS-direktivet även åtgärder på nationell nivå. Dessa handlar bland annat om att ta fram en nationell strategi för säkerhet i nätverks- och informationssystem, upprätta en nationell enhet för hantering av IT-säkerhetsincidenter, nationella behöriga myndigheter och en gemensam kontaktpunkt samt om att delta i europeiska samarbetsgrupper.

Spola sedan fram bandet några år så kan man konstatera att det första NIS-direktivet och dess krav, incidentrapporteringen och samarbetsformerna definitivt hjälpt till att höja nivån på informations- och cybersäkerheten i unionen. Europaparlamentet och Europeiska unionens råd menar dock att trots direktivets många framgångar så har översynen av direktivet visat på att det inte är tillräckligt för att effektivt kunna hantera utmaningarna inom cybersäkerhetsområdet. Detta är ett av skälen till att EU nu väljer att anta direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen – det så kallade NIS2-direktivet.

Eftersom NIS2 kan ses som en uppdatering av det ursprungliga NIS-direktivet kommer många av kraven som ställs i NIS-direktivet att kvarstå men kompletteras med bland annat högre krav på säkerhet och rapportering, tydligare krav på säkerhet i leveranskedjan och tydligare ansvar för personer i ledningen. NIS2 kommer även att inkludera fler sektorer och striktare tillsynsåtgärder. Målet är att ytterligare öka säkerheten och förbättra samarbetet mellan EU:s medlemsländer. Om organisationer inte uppfyller kraven i NIS2 kan de drabbas av sanktionsavgifter.

Några av kraven som behöver uppfyllas enligt NIS2 är:

•Strategier för riskanalys

•Hantering av incidenter

•Planer för verksamhetskontinuitet

•Säkerhet vid anskaffning, utveckling och förvaltning

•Strategier och rutiner för att bedöma effektiviteten i riskhanteringsåtgärder

•Utbildning i informationssäkerhet

•Åtkomstkontroll och hantering av tillgångar

•Lösningar för multifaktorsautentisering

•Strategier och rutiner för kryptografi

•Säkerhet i leveranskedjan

För att uppfylla kraven i det första NIS-direktivet menar MSB i sina föreskrifter (MSBFS 2018:8) att varje leverantör ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna ISO 27001 och ISO 27002 eller motsvarande. Det är troligt att ett arbetssätt enligt ISO 27001 kommer att vara en bra grund för att efterleva kraven även i NIS2.

Jämfört med det första NIS-direktivet har omfattningen utökats avsevärt med flera och bredare sektorer. Ytterligare en förändring är att sektorerna nu även delas in i två kategorier – så kallade högkritiska sektorer som listas i bilaga I till direktivet, samt andra kritiska sektorer som listas i bilaga II.
De högkritiska sektorerna är:

•Energi (elektricitet, fjärrvärme, fjärrkyla, olja, gas, vätgas)

•Transporter (lufttransport, järnvägstransport, sjöfart, vägtransport)

•Bankverksamhet

•Finansmarknadsinfrastruktur

•Hälso- och sjukvårdssektorn

•Dricksvatten

•Avloppsvatten

•Digital infrastruktur (leverantörer av internetknutpunkter, DNS-tjänster, molntjänster, datacentraltjänster, nätverk för leverans av innehåll, registreringsenheter för toppdomäner, tillhandahållare av betrodda tjänster, allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster)

•Förvaltning av IKT-tjänster (leverantörer av hanterade tjänster och säkerhetstjänster)

•Offentlig förvaltning (nationell och regional nivå – Huruvida kommuner ska omfattas är en fråga som den nationella utredningen ska titta på.)

•Rymden (operatörer av markbaserad infrastruktur)

De som listas som andra kritiska sektorer är:

•Post- och budtjänster

•Avfallshantering

•Tillverkning, produktion och distribution av kemikalier

•Produktion, bearbetning och distribution av livsmedel

•Tillverkning (medicintekniska produkter, datorer, elektronikvaror, optik, elapparatur, motorfordon, släpfordon och påhängsvagnar, andra transportmedel och övriga maskiner)

•Digitala leverantörer (onlinemarknadsplatser, sökmotorer, plattformar för sociala nätverkstjänster)

•Forskning (I vilken utsträckning universitet och högskolor kommer att omfattas är en fråga som den nationella utredningen ska titta på.)

Det är dock inte samtliga organisationer i alla sektorer som listas ovan som omfattas utan enbart de som betecknas som medelstora företag eller större. Gränsvärdena för vad som anses vara medelstora företag är 50 personer och en årsomsättning eller balansomslutning på 10 miljoner euro.

Det finns flera undantag från storlekskraven som gör att organisationer som inte uppnår dessa ändå kan omfattas. Bland annat om en störning av tjänsten som tillhandahålls kan ha betydande påverkan på människors liv och hälsa, om organisationen är den enda leverantören av tjänsten i en medlemsstat eller om en störning på tjänsten skulle kunna medföra gränsöverskridande systemrisker.

På grund av att NIS2 innehåller krav på säkerhet i leveranskedjan är det inte bara de verksamheter som omfattas som kommer att påverkas utan även deras leverantörer och underleverantörer. På så sätt kommer NIS2 att få betydligt vidare påverkan än enbart på de sektorer som explicit anges i direktivet.

I det första NIS-direktivets implementering i Sverige angavs att det var verksamheterna själva som var ansvariga för att identifiera om de omfattades eller inte. Stöd för organisationer att identifiera om de omfattas finns i MSB föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2021:9) samt i förekommande fall i tillsynsmyndigheternas föreskrifter. Föreskrifterna specificerar de olika sektorerna ytterligare och vilka kriterier som behöver uppfyllas för att omfattas. Om man som verksamhet anser sig omfattas anmäler man sig till berörd tillsynsmyndighet för sin sektor. Anmälningsförfarandet skiljer sig rent praktiskt åt något mellan tillsynsmyndigheterna men går i stort ut på att man anmäler in ett antal uppgifter om sin verksamhet inklusive kontaktuppgifter.

I regeringens direktiv till utredningen om implementeringen av NIS2 står det att samma princip gällande identifiering och anmälning bör vara utgångspunkten även förNIS2 men att utredningen bland annat ska föreslå hur entiteter som omfattas av regleringen ska identifieras och registreras.

NIS2 antogs i december 2022 och medlemsländerna ska nu implementera NIS2 i nationell lagstiftning. Regeringen har beslutat om att tillsätta en utredning för att föreslå de anpassningar av svensk rätt som krävs för att NIS2 ska kunna genomföras. Utredningen ska lämna sitt svar senast den 23 februari 2024 innan direktivet ska börja gälla under hösten 2024.

Martin Palmqvist

Senior informationssäkerhetsrådgivare på Secify. Tidigare bakgrund inom flera olika statliga myndigheter, bland annat Regeringskansliet och Myndigheten för samhällsskydd och beredskap. Det roligaste med yrket är hur omväxlande det är med ett stort behov hos verksamheter och många strategiska och komplexa utmaningar.

Infosäkkollen – en termometer för informationssäkerhetsarbete

Som en följd av de senaste årens försämrade säkerhetsläge i omvärlden och en enorm ökning i antal attacker från cyberkriminella har lagstiftningen inom informationssäkerhetsområdet stärkts upp betydligt. Bland annat med införandet av GDPR, förändringar i Säkerhetsskyddslagen och NIS I- och NIS-II-direktiven. Samtidigt pågår ett stort arbete inom EU för att stärka informationssäkerhetsarbetet inom energisektorn. Allt detta ställer högre och skarpare krav på verksamheternas arbete med informationssäkerhet.

Som en del i att förstärka informationssäkerheten i offentlig sektor fick Myndigheten för samhällsskydd och beredskap (MSB) år 2019 ett regeringsuppdrag att ta fram verktyg för att följa upp det systematiska informationssäkerhetsarbetet. Ett delresultat av uppdraget blev verktyget Infosäkkollen som riktar sig till kommuner, regioner och statliga myndigheter för att stödja deras förbättringsarbete inom informationssäkerhetsområdet.

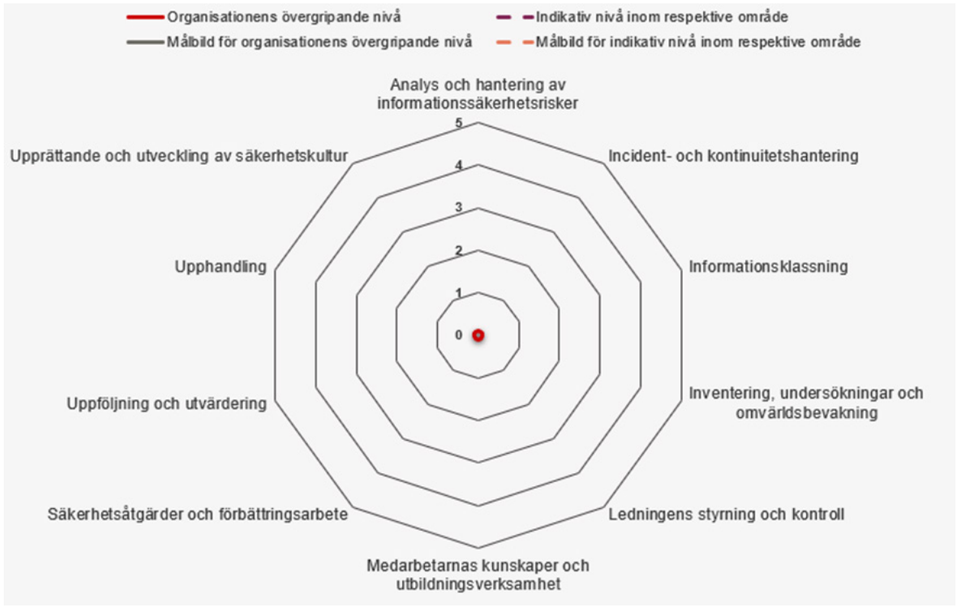
Infosäkkollen är uppbyggt utifrån MSB:s föreskrifter och stöd, som i sin tur bygger på standardserien ISO/IEC 27000. Verktyget ger stöd till uppföljning på en strategisk nivå och efter att man genomfört Infosäkkollen visar resultatet i vilken utsträckning organisationen bedriver ett systematiskt informationssäkerhetsarbete. Statliga myndigheter är skyldiga att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete enligt MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2020:6). Men även organisationer som inte omfattas av föreskrifterna kan använda dem som stöd för arbetet och för att hitta rätt ambitionsnivå för sitt interna informationssäkerhetsarbete.

En av poängerna med att använda Infosäkkollen är att stärka säkerhetskulturen i verksamheten. Begreppet säkerhetskultur är ett ganska sammansatt begrepp som består av tankemönster, värderingar och beteenden hos grupper och individer. Medarbetarnas kunskaper, ledningens och kollegernas signaler samt hur individens arbetssituation ser ut är några exempel på faktorer som påverkar resultatet av informationssäkerhetsarbetet.

Med hjälp av Infosäkkollen får verksamheten en återkoppling om vilken nivå organisationen befinner sig på och vilka utvecklingsområden som är viktiga att fokusera på för framtiden. De 10 delområden som Infosäkkollen belyser är:

- analys och hantering av informationssäkerhetsrisker
- incident- och kontinuitetshantering
- informationsklassning
- inventering, undersökningar och omvärldsbevakning
- ledningens styrning och kontroll
- utbildningsverksamhet och medarbetarnas kunskaper
- säkerhetsåtgärder och förbättringsarbete
- uppföljning och utvärdering
- upphandling samt
- upprättande och utveckling av säkerhetskultur

Efter man genomfört Infosäkkollen ska kommuner, regioner och statliga myndigheter rapportera in sina resultat till MSB, som ställer samman svaren. Verktyget ger direkt återkoppling på vilken nivå man ligger, men tack vare MSB:s sammanställning är det möjligt att jämföra sitt resultat med andra liknande



Spindeldiagram som visar organisationens resultat inom varje delområde när man genomfört Infosäkkollen. Finns också möjlighet att visa organisationens målsättningar.

verksamheter.
Informationssäkerhet är ett gemensamt ansvar för hela organisationen. Säkerhet är en förutsättning för att man ska kunna använda sin information på avsett sätt och med hjälp av den nå sina mål. Att bedriva ett systematiskt arbete med informationssäkerhet betyder att det finns en tydlig och strukturerad styrning som grundar sig i ledningens vision och mål. Det övergripande syftet med ett systematiskt informationssäkerhetsarbete är att ge informationen rätt skyddsnivå och genom ständiga förbättringar anpassa sig till förändringar i omvärlden.

De grundläggande stegen vid allt systematiskt informationssäkerhetsarbete är att:

- identifiera sina informationstillgångar

- värdera informationstillgångarna utifrån konfidentialitet, riktighet och tillgänglighet

- bedöma vilka risker som kan förekomma när informationstillgångarna hanteras

- införa ändamålsenliga och proportionerliga säkerhetsåtgärder

Så arbetar man med Infosäkkollen

Infosäkkollen är i grunden byggt i Excel. Kärnan är ett formulär med frågor som belyser centrala delar av det systematiska informationssäkerhetsarbetet utifrån de 10 delområdena.
Man samlar in underlag, så brett som möjligt, från olika delar av organisationen. Ett bra sätt att samla in den nödvändiga informationen är en workshop där olika funktioner och roller deltar. Informationssäkerhetssamordnaren kan med fördel hålla ihop arbetet, men det är inte avgörande. Det viktigaste är att det samlade svaret förankras hos ledningen för att få upp informationssäkerhetsfrågan på rätt nivå i organisationen. Förankringen i ledningen gör man lämpligen genom att baka in resultatet från Infosäkkollen i Ledningens Genomgång som man bör genomföra en gång per år (om organisationen arbetar enligt ett LIS baserat på ISO 27001)

Verktyget delar in det systematiska informationssäkerhetsarbetet i fyra nivåer, som är tänkta att svara mot ett stegvis utvecklingsarbete:

Nivå 1: Organisationer som har grunderna i informationssäkerhetsarbetet på plats, åtminstone i begränsad utsträckning

Nivå 2: Organisationer som bedriver informationssäkerhetsarbetet med en viss systematik, och som är bättre på grunderna än på nivå 1.

Nivå 3: Organisationer som har ett kvalificerat innehåll i sitt informationssäkerhetsarbete, och som är bättre på både grunderna och systematiken än på nivå 2.

Nivå 4: Organisationer som arbetar avancerat med ständiga förbättringar, samt är bättre på såväl grunderna som systematiken och innehållet än på nivå 3.

Direkt när man har fyllt i svaren ger Infosäkkollen svar på vilken nivå av 1–4 organisationen befinner sig och vilka områden som behöver utvecklas. Verktyget ger en översiktsbild som man kan använda som underlag för diskussion i till exempel ledningsgruppen.

Gemensamt för alla nivåer är att de bygger vidare på och fördjupar innehållet från föregående nivå. Till exempel har en organisation på nivå 2 inte bara utvecklat viss systematik i sitt arbete utan också kommit längre med informationssäkerhetens grunder än en organisation på nivå 1.
Frågorna på den lägsta nivån mäter om organisationen har de grundläggande delarna i informationssäkerhetsarbetet på plats. Frågorna undersöker bland annat:

- om ledningen är engagerad i informationssäkerhetsarbetet

- om organisationen har inventerat sina informationstillgångar

- om organisationen har infört arbetssätt på centrala områden (som tex informationsklassning och riskhantering)

- om organisationen har undersökt medarbetarnas kunskaper inom informationssäkerhetsarbete.

Att ledningen tar kontroll över arbetet med informationssäkerhet är avgörande för resultatet. Återkommande uppföljningar och utvärderingar av arbetets olika delar är också ett centralt underlag i styrningen. Att arbeta systematiskt innebär att man arbetar medvetet och metodiskt genom de olika LIS-stegen Planera, Genomföra, Följa upp, Utvärdera och Förbättra.

Konkret innebär det att organisationen, för de olika delarna i informationssäkerhetsarbetet:

- medvetet väljer arbetssätt, till exempel beslutar och dokumenterar om riktlinjer, rutiner, instruktioner, modeller eller verktyg

- implementerar och tillämpar arbetssätten i alla relevanta

situationer och verksamhetsprocesser

- regelbundet följer upp resultaten av arbetssätten

- utvärderar och förbättrar arbetssätten.

Uppföljningen med Infosäkkollen avser de senaste två åren, därför kommer nyligen genomförda åtgärder och förbättringar inte att få fullt genomslag i återkopplingen från Infosäkkollen. Själva nyttan med resultatet handlar om att se framåt. Tanken är att få ett underlag till arbetet med ständiga förbättringar, och att främja en positiv uppföljningskultur över tid, snarare än att fokusera på resultatet i sig. Att mäta systematiskt informationssäkerhetsarbete är komplext och kan göras på väldigt många olika sätt. Men den återkoppling som ges av Infosäkkollen ger en kvalificerad bedömning utifrån svaren i de 10 olika delområdena.

Resultatet av organisationens arbete med riskanalys ska naturligtvis användas vid valet av säkerhetsåtgärder, men också som underlag för att utforma medarbetarnas utbildning. Informationssäkerheten i organisationen påverkas inte bara av de olika arbetsmomenten i informationssäkerhetsarbetet och de tekniska eller administrativa säkerhetsåtgärder som införs. Även säkerhetskulturen i organisationen spelar en viktig roll för att både det systematiska arbetet och skyddet ska fungera.

Analys

När man genomfört Infosäkkollen och påbörjar sin analys så presenterar verktyget ett sammanfattande spindeldiagram. Tillsammans med stapeldiagram, som visar uppfyllnadsgrad i procent, för vart och ett av de 10 delområden ger detta en bild av organisationens nivåuppfyllnad. Med hjälp av detta kan man sedan jämföra resultat mellan olika år för att fånga och visa på de förflyttningar som gjorts i organisationen.
I Infosäkkollens flik för ”Analysstöd” kan man redogöra för hur man själv ser på resultatet samt plotta ut målbilden för de kommande två åren. Denna information ska i huvudsak användas internt och den kan med fördel kommuniceras i en presentation till ledningsgruppen.

Det är viktigt att komma ihåg att modellen bara kan ge en indikation om vilken nivå man ligger på, den är inte tänkt att omfatta hela MSB:s författning eller alla sätt som kraven kan uppnås på. Till exempel berör modellen inte fysiskt skydd. Den mäter heller inte hur organisationens arbete förhåller sig till specifika krav i andra författningar, exempelvis dataskyddsförordningen eller säkerhetsskyddslagen.

Säker och osäker bedömning

För varje fråga behöver man avgöra hur säkert eller osäkert svaret eller svaren är. Det kan vara en fördel när organisationer har goda skäl att tro, men inte helt säkert vet, att en viss del av det systematiska informationssäkerhetsarbetet ser ut på ett visst sätt. Om man kryssar i flera svarsalternativ betyder ”Säker bedömning” att det finns dokumenterade och tydliga belägg för alla valda svarsalternativ. Alla frågor i Infosäkkollen handlar om den senaste tvåårsperioden, eftersom nivån på organisationens informationssäkerhetsarbete är resultatet av arbete och val som har gjorts över tid. Då både förändringar och uppföljning tar tid att genomföra blir det inte effektivt att mäta för ofta. Det är också en fördel att mätperioden sammanfaller med hur ofta uppföljningen genomförs. Man kan få positiva effekter om man lyckas integrera uppföljningen av informationssäkerhetsarbetet med verksamhetens övriga uppföljningar av kvalitet och ekonomi. Om man lyckas med det så blir inte informationssäkerhet ett eget område, utan en komponent tillsammans med andra, som också ska följas upp.

Sundsvalls kommun

Camilla Eriksson är informationssäkerhetssamordnare, placerad på Kommunstyrelsen i Sundsvall. Där har man använt Infosäkkollen för att stärka kommunens systematiska informationssäkerhetsarbete. Hon har sammanställt resultatet för alla förvaltningar och kommunala bolag. Därefter hon hållit genomgångar med ledningsgrupperna på kommunkontoret och i ledningsgruppen för Stadsbacken, som koncernen med de kommunala bolagen heter.Överlag är hon väldigt nöjd med Infosäkkollen: ”Det är ett bra verktyg som är enkelt att använda. Tack vare att det är byggt i Excel, behövs inga fräsiga applikationer. Användningen blir ganska självförklarande och man får enkla och tydliga resultat.”

Camilla Eriksson tycker att det är en fördel att kunna skicka ut en separat kopia av Infosäkkollen till varje nämnd och bolag så att de själva kan driva sin utveckling, med stöd från hennes roll, som centralt placerad informationssäkerhetssamordnare. När nämnderna och bolagen svarat har Camilla sammanställt en separat rapport för nämnderna och en för bolagen. Tyvärr blir ofta uppföljningen och återkopplingen på lokal nivå eftersatt på grund av att det inte finns tillräckligt med kvalificerade resurser. Trots detta så anser Camilla att Infosäkkollen väl fyller sitt syfte och bidrar till att öka medvetenheten om informationssäkerhet bland medarbetarna och att föra upp frågorna på ledningsnivå.

Personligen anser jag att det är relativt vanligt med en okunskap om risker och informationssäkerhet bland företag och myndigheter. Jag tycker det är viktigt med en tydlighet i organisationerna när det gäller ansvar och roller. Där är Infosäkkollen ett tillräckligt bra verktyg som bidrar till att stärka företags och myndigheters arbete med informationssäkerhet.

Infosäkkollens upplägg med att brett samla in information om policydokument, regler, attityder och arbetssätt m.m. inom en organisation medverkar väldigt bra till att uppmärksamma frågor om informationssäkerhet och föra upp dem på ledningens bord. För i slutändan är informationssäkerhet vanligen inte en ledningsfråga – förrän det blir det. Och då riskerar verksamheten dryga sanktionsavgifter eller störningar i sin verksamhet, som en följd av allvarliga incidenter på grund av att arbetet kommit igång för sent.

Mats Österlund

Roll/Yrke: Konsult inom informationssäkerhet

Arbetsplats: Arkiv IT

Har jobbat med IT i många olika former sedan slutet av 1990-talet. Med informationssäkerhet sedan 2017. Har för närvarande uppdrag som informationssäkerhetsstrateg på Region Värmland.

På fritiden är han en inbiten skogs- och fjällvandrare, seglare. Åker gärna till alperna för skidåkning.

KLASSA – dokumentation av kommunala och regionala processer

Klassificeringssystemet Klassa är ett centralt instrument för att med utgångspunkt i en upparbetad kunskap om verksamhetens processer bygga ett underlag för den elektroniska informationsförvaltningen – värdering av informationen på kort och lång sikt, riskanalys och säkerhetsklassning, beslut om vad som bör dokumenteras, hur det ska dokumenteras och hur dokumentationen ska hanteras. Men Klassa får inte bli ett verktyg för enbart informationsförvaltare. Värdet av Klassa består i att det är av värde även för andra i organisationen.

I mitten av 1980-talet nåddes vi av rykten om att man i Australien bytte arkivperspektiv – från det traditionella organisatoriska perspektivet till ett som utgick från en beskrivning av organisationens verksamhet. När jag långt senare fick tillfälle att fördjupa mig i detta förstod jag att det gällde utvecklingen av Commonwealth Record Series (CRS) från 1960-talet till ett system som tillät registrering av funktioner och aktiviteter. Syftet med detta var att hitta en redovisningsform som kunde bestå även vid de allt tätare organisationsförändringarna.

I skriften ”Den goda visionen” (Svenska kommunförbundet 1992) lades detta synsätt till grund för ordningen i ett så kallat kontorsinformationssystem där metadata som beskrev ”funktioner” och ”aktiviteter” skulle speglas i arkivets mappstruktur.

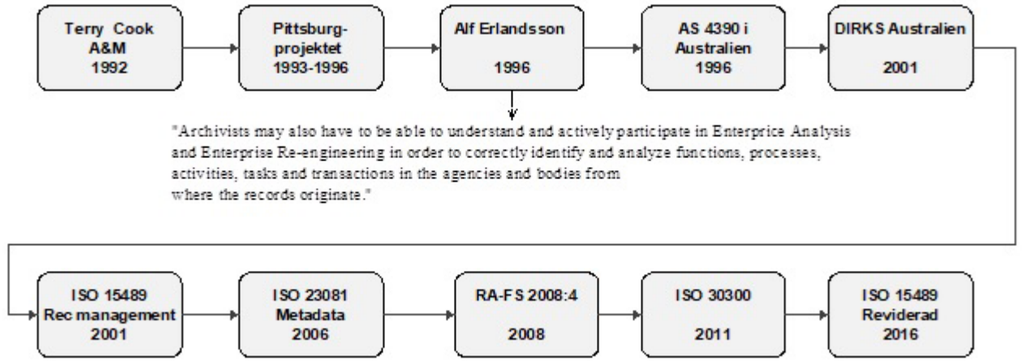
”En struktur för KI-systemet bör därför enligt vår mening inte baseras på den för tillfället gällande organisationen. KI-strukturen bör i stället byggas upp så att den avspeglar kommunens/myndighetens faktiska verksamhet. Med verksamhet avses här de arbetsuppgifter myndigheten utför med stöd av lag, annan bestämmelse eller uppdrag... Inom varje myndighet bör KI-systemet ges en struktur som svarar mot en riktig beskrivning av myndighetens verksamhet.”

Det handlade om strukturen i det elektroniska arkiv vi såg växa fram och det stod klart att det gamla allmänna arkivschemat var på väg ut. Internationellt fortsatte utvecklingen under 1990-talet med en omfattande diskussion om ”electronic records” och påbörjat arbete med standarder som kopplade records till function – eller processer, som blev den svenska översättningen. I den australiensiska standarden AS 4390 år 1996 lades grunden för den analysmetodik och de begrepp som utmynnade i standarden för records management ISO 15490 år 2001, standarden för processanalys ISO 26122 år 2008 och Ledningssystemet för verksamhetsinformation (ISO 30300-familjen) år 2011.

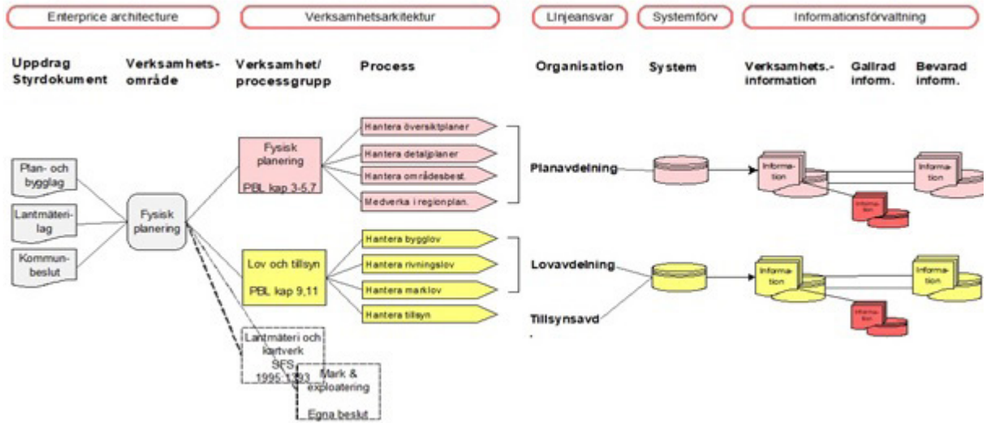
Steg för steg nådde denna utveckling även våra breddgrader. I Sundsvalls kommun publicerade vi år 1987 en verksamhetsbaserad arkivkatalog för tiden 1863-1985 och från 2005 upprättade vi processbaserade dokumenthanteringsplaner. Vi förstod vid det laget betydelsen av standarder för records management och jag var själv involverad i bokprojekt i NLA:s regi år 2000 och 2005 där sådant beskrevs. En avgörande milstolpe var dock att Riksarkivet utfärdade RAFS 2008:4, där statliga myndigheter ålades upprätta ett schema för klassificering av verksamhetens processer samt ordna arkiven enligt den processuella strukturen.

2. På jakt efter processerna - Klassa

Samrådsgruppen för kommunala arkivfrågor mottog under denna tid ofta frågor om en kommunal struktur för verksamhetsklassificering och år 2012 fick jag Samrådsgruppens uppdrag att utarbeta förslag till en sådan. Arbetet bedrevs i dialog med en referensgrupp och utmynnade i det Klassa som publicerades våren 2013.



Utveckling av standarder för hantering av verksamhetsinformation



Uppdrag - verksamheter - processer

En central uppgift blev nu att identifiera alla de processer som bedrivs i kommuner och regioner och placera dessa i en struktur som speglar verksamhetens organisering. Vi sneglade ordentligt på kommunförbundets och SCB:s mycket stabila statistikområden - i bruk sedan 1800-talets slut – liksom de diariedossiéplaner som underhölls av Svenska kommunförbundet 1958–1989. Vårt ändamål var emellertid bredare än dessa, vi sökte en struktur som kunde användas för alla slags informationsmängder i kommun och landsting – en struktur som innefattade ledning, styrning och kärnverksamheter och där beskrivningen av kärnverksamheterna vilade på kunskap om de faktiska arbetsprocesserna, identifierade i anslutning till de kommunala uppdrag som formuleras i lagstiftningen.

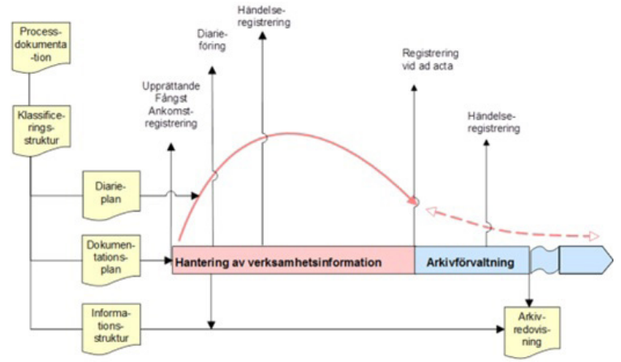
Relationen mellan uppdrag, verksamhetsområde och process och den verksamhetsinformation som hanteras i processen är och förblir ett huvudspår som måste analyseras och beskrivas i alla sammanhang där man organiserar sin informationsförvaltning. Grafen illustrerar detta förhållande.

Principer i Klassa

När man arbetar med ett system som har ”riks”ambitioner måste man eftersträva systematik och konsekvens och de begrepp som används måste vara definierade. Vår målsättning var naturligtvis att nå fram till en lösning som alla kommuner/ regioner kunde tillämpa och helst också gilla – men vi var också medvetna om att många kommuner skulle välja en ”enklare” lösning. Jag sammanfattar nu de saker som utmärker Klassa – egenskaper som förklarar varför vissa valt Klassa; sannolikt också varför vissa valt att gå egna vägar.

1. Huvudstruktur och övergripande ledning
Schemat har en huvudindelning som består av 1. Ledning, 2. Stöd och 3. Kärnverksamhet. Var och en av dessa underindelas i Verksamhetsområde, Processgrupp och Process. Med 1. Ledning avses inte ledning i allmänhet utan kommunledning och förvaltningsledning, dvs de processer som krävs för att leda hela förvaltningen/nämnden/kommunen.

2. Funktionsledning
Varje nivå av schemat inleds med en 0-grupp som rubrikeras Ledning-Styrning-Organisering. Där beskrivs de processer som har att göra med varför och på vilket sätt verksamheten bedrivs - hur styrdokument ska upprättas och tillämpas, hur den planeras, hur den resurssätts, hur den följs upp. Funktion är ett svårt begrepp. Här avses inte organisatoriska funktioner utan verksamhetsfunktioner.



I kvalitetssammanhang brukar dokumentation på detta område kallas styrande dokument.
Exempel på en sådan dokumentation kan vara ordning för brandsläckning.

3. Genomförandeprocesser
Genomförandeprocesserna (processgrupper och processer) är de processer där den resurssatta verksamheten är i arbete, dvs när varan/tjänsten produceras.
I kvalitetssammanhang brukar dokumentation på detta område kallas redovisande dokument.
Exempel på en sådan dokumentation kan vara redogörelse för aktiviteter som bestått i att hantera operativ brandbekämpning.

4. Verksamhetsstödets struktur
Bland de olika klassificeringsscheman som upprättats under senare år finner man många som inleds med ”Personal” och ”Ekonomi” men som helt saknar de processer som tillhör informationsförvaltningen. I Klassa ligger de senare överst i verksamhetsstödet, tillsammans med systemförvaltning och arkitektur. Verksamhetsstödet i Klassa skiljer ut å ena sidan de verksamhetsstöd som krävs för långsiktig förmåga att utföra uppgiften, å andra sidan de som bildar det organisatoriska skalet.

5. Kärnverksamhetens struktur
Kärnverksamheterna innefattar 8 kommunala och 5 regionala verksamhetsområden. Kommunernas och regionernas utbildnings- och kulturverksamheter hålls alltså åtskilda.

3. Tillämpning och nuläge Genomslag

Vi ha tyvärr inga uppgifter om hur många kommuner och regioner som använder Klassa. Mitt intryck är att det är många och kanske är Klassa nu det system som är mest spritt. Många använder Klassa utan att i alla delar följa de principer som beskrivits ovan. Att lokalt anpassa Klassa till det arbetssätt som råder i den egna kommunen är dock inte fel - en vinning med Klassa är att man kan använda systemet som utgångspunkt för sitt eget analysarbete, ett förslag att ta spjärn mot och som genom att det existerar gör det egna arbetet så mycket enklare.

Förvaltning 2013–2023

Klassa ägs av beställaren, Samrådsgruppen för kommunala arkivfrågor, men någon aktiv förvaltning från Samrådsgruppens sida förekommer inte i dagsläget. Mitt företag och Rundström konsult AB gjorde år 2018 en översyn som ledde fram till nu aktuella Klassa 2.0. För närvarande finns Klassa 2.0 publicerat på Samrådsgruppens hemsida och på den hemsida för informationsförvaltning som drivs av Näringslivets arkivråd (www.informationsforvaltning.com).

4. Processdokumentation – för informationsförvaltare och övriga intressenter

Klassa har skapats som ett instrument för modern informationsförvaltning, ett sätt att redovisa verksamhetsinformation där allmänna arkivschemats arkivstruktur ersätts med en struktur som representerar den faktiska verksamheten.
Det är viktigt att den förvaltade processtrukturen läggs till grund för en informationsförvaltning där samma struktur återkommer i ärenderegistrering, dokumentationsplanering, gallringsbeslut och arkivredovisningar.

”Informations-Klassa” och ”Säkerhets-Klassa”

Det är också angeläget att förse processdokumentationen med metadata och beskrivningselement som handlar om informationssäkerhet på processnivå – riskanalyser, säkerhetsklassningar, uppgifter om integritetsskydd och sekretess. Om processdokumentationen i Klassa utrustas med information av detta slag då erhåller kommunernas informationsförvaltare ett ovärderligt instrument för sitt arbete. De behöver t ex inte vänta i åratal på att någon kompetent säkerhetsexpert utför riskanalyser och arrangerar för säkerhet - ty allt sådan ligger med i det paket som är framtidens Klassa och som kan användas om utgångspunkt i det lokala arbetet.

Ett par år efter lanseringen av Klassa framkom dock att SKR lanserat ett annat Klassa, för enkelheten skull här kallat Säkerhets-Klassa - ett instrument för riskanalys och säkerhetsklassning som även beskrivs på SKR:s hemsida. Säkerhets-Klassa är fokuserat på system och systemmiljöer, men riskanalysverktyget kan även tillämpas på dokumenterade processer.

Att SKR och Samrådsgruppen inte lyckats åtgärda den irriterande namngemenskapen är anmärkningsvärt. I den dialog som pågått om dessa saker har dock framkastats en idé om att Informations-Klassa och Säkerhets-Klassa borde byggas samman till ett gemensamt verktyg som hanterar både processdokumentation och dokumentation av riskanalyser och säkerhetsklassningar. För oss som arbetar med inspiration från Ledningssystem för verksamhetsinformation, LVI (ISO 30300-familjen) är det självklart att hantera informationssäkerheten som en avgörande funktion i informationsförvaltningen. Analysmodellen i Ledningssystem för informationssäkerhet, LIS (ISO 27000-familjen) utgår liksom LVI från den dokumenterade processen. Riskanalys och säkerhetsklassning enligt LIS sker med andra ord med samma underlag som informationsvärdering och planerade arkivåtgärder enligt LVI. En sammanslagning skulle kunna utmynna i ett system med tre delar

• manual för processkartläggning och processdokumentation

• manual för riskanalys och säkerhetslassning

• förslag till standardiserat klassificeringsschema (”Klassa”) som innefattar resultat av riskanalys och säkerhetsklassning

Redskap för övriga intressenter inklusive Inera

Klassa innehåller väldigt lite information om hur processerna drivs och fungerar. Den väldokumenterade och beskrivna arbetsprocessen är en neutral plattform som kan delas med alla aktörer i organisationen: informationssäkerhetsansvariga, arkitekter, it-strateger, arkivarier, kvalitetsansvariga m fl. Den kan utgöra denna plattform eftersom den arbetar på neutral mark - den beskriver helt enkelt vad som uträttas. En förutsättning för att den ska kunna fylla denna bredare funktion är dock att den förses med beskrivningar av hur processen drivs och ett antal beskrivningselement som nu saknas.

Inom Inera och den organisation som kallas Arkitekturgemenskapen pågår ett arbete med beskrivning, kartering och klassificering av ”förmågor”. Vad är då en förmåga och vad är syftet med detta koncept? En förmåga är helt enkelt ett uppdrag och en kapacitet att utföra detta uppdrag. Vi kommer här mycket nära det som ryms i Klassas 0-signerade ledningsfunktion: de aktiviteter som styr hur genomförandeprocessen ska utformas och hanteringen av de resurser som krävs. Inera har använt Klassa 2.0 som underlag till sin förmågekarta, men med ganska stora förändringar i strukturen. Det avgörande är dock att Arkitekturgemenskapens arbete inte uträttas för strukturens skull eller för att åstadkomma en god informationsförvaltning – utan för att standardisera ett bra sätt att lösa uppgiften – t.ex. att genomföra en hjärtoperation. Det är alldeles utmärkt. Om detta existerat när vi byggde Klassa hade vi använt det. Arkitekturgemenskapen och Inera är instrument i det kommunala digitaliseringsarbetet. Förmågebeskrivningen och förmågeutvecklingen är ett led i detta. Vi påminns om att digitaliseringen – som alltid – drivs av behovet av verksamhetsutveckling.

Ett bredare och djupare Klassa

Ett Klassa som fyller de funktioner jag nu beskrivit borde förses med följande beskrivningselement:

• beskrivningar av aktiviteter och transaktioner, med eller utan grafiskt stöd - ett viktigt led i processtyrningen, för effektivitet och kvalitet; helt avgörande för verksamhetsansvariga och utvecklare

• styrdokument kopplade till uppdraget - har stor betydelse för de varor och tjänster som produceras och hur informationen ska värderas

• dokumentationskrav för den verksamhet som beskrivs - blir styrande för hur verksamhetsinformation skapas och förvaltas i processen

• relationen till andra processer (vertikalt, horisontellt) - bidrar till förståelse för processens natur och är avgörande för schematisering och klassificering, dvs verksamhetsmetadata

• behov hos externa intressenter - bidrar till värdering för bevarande

• riskanalys och säkerhetsklassning på processnivå - avgörande för informationssäkerhetsarbetet

• värdering för bevarande på processnivå - avgörande för beslut om kvarhållande och bevarande

• koppling till systemmiljö inklusive applikationer - viktigt för teknisk proveniens över tid

• uppgift om ansvarig administrativ enhet - representerar en viktig kontextuell metadata

Sammantaget skulle ett ”Klassa” med detta innehåll kunna bli en gemensam resurs för hela organisationen – inte bara en resurs för informationsförvaltarna.

5. Ett pågående vägval

Samverkan - eller skilda vägar?

Säkerhets-Klassa backas upp av SKR och Inera/Arkitekturgemenskapen mönstrar ett stort antal verksamhetsarkitekter i hela landet i ett arbete som bedrivs i samverkan med DIGG och SKR. I detta arbete riskerar Informations-Klassa steg för steg att marginaliseras. Men att Informations-Klassa inte förvaltas aktivt varken av Samrådsgruppen eller av SKR och att Säkerhets-Klassa hanteras som om Klassa inte existerade är uttryck för ett ålderstiget synsätt i en förlegad organisationskultur. Vi riskerar nu än en gång få uppleva hur kommunernas och regionernas informationsförvaltning förpassas bort från händelsernas mitt; att det klassificeringssystem vi bidragit till att utveckla, det system nota bene som skulle möjliggöra ett samlat grepp om de olika funktioner som nämnts, blir ett system för de som arkiverar och de som sköter arkivet. En sådan ordning representerar det förgångna.

Det är sammanfattningsvis angeläget att Klassa utvecklas och drivs i samverkan med de olika intressenter som jag beskrivit och att harmonisering eftersträvas. Så – och endast så – kan vi uppnå att framtida verksamhetsinformation och hanteringen av denna i olika miljöer blir en gemensam angelägenhet för hela organisationen och ett led i dess uppgift att producera varor och tjänster.

Klassa 2.0 finns tillgängligt på

Samrådsgruppens hemsida ***http://www.samradsgruppen.se/index.php/rad-och-stod***
NLA:s hemsida ***www.informationsforvaltning.com***

Tom Sahlén

Roll: Senior underkonsult hos ArkivIT.

Tom Sahlén har en bakgrund som arkivchef i Sundsvalls kommun men har efter 2011 arbetat som fristående konsult. Han har medverkat i en rad bokprojekt för bl. a. Näringslivets arkivråd, senast ”Informationsförvaltning i offentlig och privat sektor” (NLA 2016). Tom är upphovsman till det system för klassificering av kommunala och regionala arbetsprocesser som kallas ”Klassa” och som lanserades år 2013. Senior underkonsult i ArkivIT.

Inom räckhåll eller i molnet? Tre yrkesperspektiv på informationslagring

När vi navigerar genom den digitala transformationens virvlar, ställs vi inför en avgörande fråga: Var ska vi förvara vår mest värdefulla tillgång – informationen? Molnbaserad informationslagring, ett självklart inslag i denna diskussion, har blivit föremål för polariserade debatter mellan IT-specialister, arkivarier och dataskyddsombud. Vad som ofta går förlorat i dessa debatter är dock nyanserna – en objektiv och balanserad syn på både fördelarna samt utmaningarna som molntjänster innebär. Så kan dessa tjänster verkligen erbjuda säkra och effektiva lösningar för bevarande av information? Vi ska utforska denna fråga från olika yrkesperspektiv och ta en närmare titt på de för- och nackdelar med molnbaserade lösningar som ofta förbises.

Vi börjar med IT-specialisterna, de största förespråkarna för molntjänster. De lockas av de potentiella tids- och kostnadsbesparingar som molntjänster kan erbjuda jämfört med att förvalta egen infrastruktur. Men de överskattar ofta de faktiska vinsterna. En stor utmaning ligger i att både förstår själv och sen följa upp de GDPR- och informationssäkerhetskrav som ställs på externa leverantörer och även deras underleverantörer. Vilka rutiner och skyddsåtgärder har de på plats? Många organisationer saknar tid, kompetens och/eller vilja att granska sina leverantörer. Kan vi lita på att de levererar när det gäller? Att få tillgång till korrekt information om den egna organisationens on-premise-lagring (lagring av information på organisationens egna servrar) är å andra sidan sällan ett problem.

Sen kanske det är bäst att prata om elefanten i rummet – dataskyddsombuden med GDPR- perspektivet. Dataskyddsombuden befarar oavsiktlig exponering av personuppgifter utanför organisationen och juridiska problem med underleverantörer utanför EU. Det är förstås viktiga principer som inte ska viftas

” Arkivarier har under lång tid haft en tendens att vilja samla information på en enda fysisk plats inom organisationen. Detta förhållningssätt är förstås praktiskt men principen har vid otaliga tillfällen resulterat i omfattande förstörelse”

bort, därför lockar on-premise-lösningar denna yrkesgrupp. Men sker detta på bekostnaden av informationssäkerhet och hur påverkar det organisationens regelefterlevnad som helhet?

Ett av de grundläggande, men ofta överskuggade, syftena med GDPR är att säkerställa lämpligt skydd för information. I många fall finns det dock ett malplacerat förtroende gentemot den egna it-avdelningens kapacitet och kompetens gällande säker drift av system. Molnlagring kan i många fall erbjuda överlägsen säkerhet sett till helheten. Leverantörerna kan tillhandahålla expertis inom specifika system och plattformar på ett sätt som kan vara svårt för organisationens egna it-specialister att matcha. Till exempel kan säkerhetsuppdateringar och patchningar (mindre uppdateringar) ske löpande (snabbt) utan att behöva beställas av verksamheten vilket resulterar i kortare ledtider mellan identifiering av risker och implementering av lösningar. Därmed får man ett effektivt skydd mot den vanligaste källan till cyberattacker, eftersatta system med säkerhetsbrister.

Arkivarier med sitt fokus på långsiktigt bevarande bävar för risken att informationen ska försvinna – att lagra informationen inom organisationen känns ofta säkrare. Arkivarier har under lång tid haft en tendens att vilja samla information på en enda fysisk plats inom organisationen. Detta förhållningssätt är förstås praktiskt men principen har vid otaliga tillfällen resulterat i

omfattande förstörelse, något som illustreras i Wikipedias List of destroyed libraries. Händelserna, som varierar i omfattning och tidsram har orsakats av allt från medveten informationsförstöring till krig, naturkatastrofer och brand.

Det finns många exempel på hur den redundans som molntjänster möjliggör kan innebära en robust informationslagring. Nu finns det möjlighet att lagra kopior av information i en annan stadsdel, i en annan region eller i ett annat land. Ett aktuellt exempel kommer från Ukraina, som nyligen påbörjade en process att flytta kopior av samhällsviktiga data från offentliga institutioner till datacenter i bland annat Polen och Frankrike. Privata moln konstruerades med kryptering och nätverken säkrades för att kunna lita på både lagringen och transportering av informationen. Syftet var att skydda sina tillgångar mot fysiska och cyberangrepp. Det var en omfattade process att flytta över 150 register från olika myndigheter till molnen. Detta visade sig snabbt vara en värdefull försiktighetsåtgärd när ett regeringsdatacenter skadades av ryska missiler under krigets första dagar – ingen data gick förlorad tack vare molnbackuper.

Över lag är offentliga data och tjänster ofta strategiskt viktiga för ett lands försvar, och informationsförsörjning är därför en vanlig måltavla. Tänk hur viktigt folkbokföringsregister, skatteuppgifter och Bank-id är för det svenska samhället. Det är avgörande att sådana tjänster skyddas eftersom tillgång- och tillförlit till denna information kan påverkas på destruktiva sätt av ett anfallande land. Risken är alltså inte enbart att information kan gå förlorad, att information permanent förvanskas är också en risk.

Även Estland, känt för sin digitala framkantsposition, har omfamnat molnkonceptet genom att upprätta en ”dataambassad” i Luxemburg. Där säkerhetskopieras och bevaras kritiska databaser och tjänster, vilket ytterligare understryker vikten av redundans för långsiktigt informationsbevarande. Att lagra offentliga institutioners data utanför den egna regionen eller nationen utgör ett skydd mot existentiella hot. Detta är särskilt relevant för organisationer som hanterar strategiskt viktig information och är någonting som borde övervägas i en tid präglad av ständigt ökande cyberhot.

Framåt ser vi en växande trend mot hybridmoln och flermolnstrategier. Hybridmoln, en kombination av on-premise-datacenter och molntjänst erbjuder organisationer en balans mellan lokal kontroll och molnets flexibilitet. Dessa lösningar kan skräddarsys för att passa organisationens specifika behov och säkerhetskrav.

Så, där står vi, vid skärningspunkten mellan tradition och framtid. Molntjänster bjuder in oss till en värld av möjligheter, med sina förmågor att erbjuda redundant informationslagring, effektivitet och säkerhet. Men som med alla teknologiska framsteg, följer komplexitet och nya utmaningar. Vi kan inte bortse från riskerna med exponering av känsliga data, juridiska svårigheter eller utmaningar med revision av underleverantörer. Som ofta är fallet, finns det ingen universallösning. Varje organisation måste granska sina specifika behov, risktolerans och kapabilitet för att avgöra hur, och i vilken omfattning de ska använda molntjänster.

Så vad har vi kommit fram till då? Det som känns viktigast att påpeka är att det finns flera dimensioner av denna fråga och att det finns både fördelar och nackdelar från alla berörda yrkesgruppers perspektiv. Framöver hoppas jag på en mer informerad, mångsidig och konstruktiv debatt rörande molnlagring så att vi inte kastar ut barnet med badvattnet.

https://en.wikipedia.org/wiki/List_of_destroyed_libraries
https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002

Andrew Tutt-Wixner

Roll: Arbete inom Arkiv, GDPR och informationssäkerhet Leksands kommun. Är född och uppvuxen i Perth, Australien innan flyttlasset tog honom bort från kuststaden till Mora via Stockholm. Till vardags arbetar han inom arkiv, GDPR och informationssäkerhet i Leksands kommun. Vid sidan av gillar han att utveckla digitaliseringsverktyg under namnet ArchiveTools.

Det han gillar allra mest inom arkiv är att arbeta med export och transformation av digitalinformation.

Informationssäkerhet stärks av öppna data

Arbete med att klassificera data som möjliga att publicera som öppna ger många fördelar. Klassificeringen är ett lämpligt första steg i arbetet med informations- och datasäkerhet, något som det ofta slarvas med. MetaSolutions Eric Hjelmestam förklarar hur det fungerar.

Cybersäkerhet, IT-säkerhet, datasäkerhet, informationssäkerhet. Det är områden med många beröringspunkter sinsemellan. Intresset för samtliga härstammar i hög grad från rädsla för att information, speciellt känslig sådan, ska komma på villovägar. Därför kan det kanske tyckas finnas en fara med att hantera, publicera och dela öppna data. ”Varför göra det lätt för utomstående att komma åt våra data, när vi vill skydda dem?”, kan man undra.

Det är synd om säkerhetsbryderier ska sätta stopp för delning av öppna data. Det innebär att man missar effektivitetsvinster i offentlig sektor, transparens för medborgare, bättre förutsättningar för näringslivet och andra fördelar som fås med öppna och delade data.

Syftet med den här texten är att förklara varför användning och publicering av öppna data inte medför sämre informationssäkerhet, utan tvärtom bidrar till ökad säkerhet. Innan vi sätter i gång är det på plats med en definition: I den här texten är begreppen information och data likvärdiga. Vilken benämning som än används handlar det om uppgifter om platser, objekt, individer, med mera, som hanteras maskinellt.

Nödvändig inventering

Det första steget i allt säkerhetsarbete som har att göra med data bör vara att ta reda på vad som behöver skyddas. Det är också det steg som det, med största säkerhet (ursäkta), slarvas mest med. De flesta organisationer har dålig koll på vilka datamängder (informationsmängder) de har, var de finns, hur känsliga de är, vem som ”äger” dem, och så vidare.

För att skydda sina data på bästa sätt behöver man veta de här sakerna. Det är, som av en händelse, också saker man behöver ta reda på för att jobba med öppna data. Det arbetet brukar benämns ”klassificering av data”. Vi kanske skulle kunna säga ”inventering av data” i stället. Hur som helst bidrar klassificering av data till att säkerhetsarbetet förenklas.

Om en datamängd en gång klassificerats som lämplig för publicering som öppna data så gäller den klassificeringen tills datamängden förändras på något avgörande sätt. Man behöver inte lägga tid och energi på att undersöka datamängden på nytt. Och man missar inte tillfällen att publicera öppna data på grund av bristande kunskap om hur datamängder är beskaffade.

Klassificering av data kan så klart låta jobbigt och komplicerat. Så kan det vara, men det behöver långt ifrån alltid vara det. Och du kan välja själv hur jobbigt och komplicerat det ska vara. Här följer ett tips för att komma i gång med klassificering av data på ett enkelt sätt.

En enda fråga

Klassificeringsarbetet börjar med att identifiera vilka datamängder som finns. Om du har tur finns det dokumenterat. Om inte kan du utgå från att medarbetare helt enkelt känner till många databaser, dokumentsamlingar och andra typer av datamängder. I vissa fall får du ägna dig åt lite teknisk arkeologi. Helt enkelt leta efter datamängder, kanske med hjälp av IT-personal.

Låt oss säga att du har tagit reda på att datamängd A finns. Nu är det dags att klassificera den. Ställ då följande fråga:

Finns det något hinder som gör att datamängd A inte kan publiceras?

Om svaret är ja lägger du datamängd A åt sidan, för vidare analys när du blivit varm i kläderna med klassificering av data. Om svaret är nej, för att du inte hittar några hinder mot publicering av datamängd A som öppna data, kan du sätta i gång med en fullständig klassificering.

Det här angreppssättet innebär att du inte behöver lägga ner en massa hårt jobb till ingen nytta när du börjar jobba med klassificering av data. Du vet att de datamängder som du lägger ner mest tid på kommer att kunna komma till användning. Tänk på att analysera en datamängd i taget. Att ge sig på samtliga identifierade datamängder på en gång kan göra att uppgiften med klassificering, i onödan, känns överväldigande.

Den vakne läsaren undrar säkert över två saker just nu:

- Vad finns det för hinder mot publicering av öppna data?
- Hur går fullständig klassificering av data till?

Låt oss besvara de frågorna, en i taget.

Tre vanliga hinder

Det kan finnas många olika hinder mot publicering av öppna data och du får lägga ner lite tid på att lära dig vilka de är. Men det är inte särskilt krångligt eller tidsödande att få grepp om det. De här tre vanliga hindren ger en uppfattning om vad det handlar om.

- En datamängd innehåller personuppgifter. Det gör i princip att det inte går att publicera en datamängd som öppen. Om det finns personuppgifter i en datamängd som du verkligen vill publicera så kan du undersöka om det går att ta bort personuppgifterna på något sätt, och publicera de data som blir kvar.
- Det är oklart hur det står till med licenser och ägandeskap för en datamängd. Vissa mjukvaruleverantörer skriver till exempel in en massa förbud mot användning av data som genereras i deras applikationer. Det finns därför all anledning att ställa krav på fri användning av data när applikationer och tjänster upphandlas.
- Det är oklart vilka personer, avdelningar och organisationer som hanterar, använder, och även äger, en datamängd. Detta bör redas ut för att undvika att någon intressent har invändningar mot publicering av data.

Om något av följande hinder manifesterar sig så vet du att du inte kan publicera en datamängd som öppna data rakt av. Du vet också att det är värt att undersöka om det finns anledning att lägga ner extra energi på att säkra datamängden.
Om du har följt processen som beskrivs ovan så har du identifierat många enklare datamängder som utan vidare analys kan publiceras som öppna data. Kvar blir de känsliga datamängderna.

De kan kräva specialister

Så här långt har vi tittat på arbetsmoment som i princip vem som helst kan utföra. När det kommer till fullständig klassificering av data kan det krävas medverkan av specialister. I vilket fall ger SKR:s webbtjänst Klassa en bra uppfattning om vad det handlar om.
Tjänsten Klassa är uppbyggd i tre delar:

”Det är synd om säkerhetsbryderier ska sätta stopp för delning av öppna data”

SKR:s webbtjänst Klassa
https://klassa-info.skr.se/demo/impactassesment

- Konfidentialitet – att informationen kan åtkomstbegränsas. De här aspekterna är de juridiskt sett mest intressanta, vad gäller att avgöra om en datamängd kan publiceras och delas som öppen.
- Riktighet – att informationen ska vara tillförlitlig, korrekt och fullständig. De här aspekterna är i praktiken lika viktiga som de juridiska. Ingen vill, eller bör, publicera och dela felaktiga data.
- Tillgänglighet – att informationen ska kunna nyttjas efter behov, i förväntad utsträckning, samt av rätt person med rätt behörighet. De här aspekterna är de som förändras när en datamängd publiceras som öppen. Tillgängligheten ökar då rejält. Vad gäller behörighet innebär publicering av öppna data att alla har behörighet till en datamängd. Krav på särskild behörighet är ett hinder mot publicering av öppna data.

Samtliga tre delar klassificeras i en av fem nivåer (nivå 0–4).

Här är ett exempel:

- Nivå 0 för konfidentialitet innebär i korthet att okontrollerad tillgång till en datamängd inte medför några risker att tala om för samhällsviktiga funktioner eller personlig integritet. Enkelt uttryckt är det fritt fram att publicera och dela som öppna data.
- Nivå 4 för konfidentialitet innebär att okontrollerad tillgång till en datamängd medför ”skada för rikets säkerhet som inte endast är ringa”. Glöm publicering och delning som öppna data.

Det varierar naturligtvis hur enkelt det är att genomföra en sådan här klassificering. I vissa fall är det uppenbart hur det ligger till. I andra fall krävs det avancerade analyser som utförs av experter.’

Datamognad på köpet
Att jobba med klassificering av data är inte bara ett sätt att möjliggöra publicering och delning av öppna data, och att öka informationssäkerheten. Det är också en nödvändig del av den digitala transformation som präglar hela samhället just nu.

Du har säkert hört att ”data är den nya oljan”, eller liknande liknelser. Du skulle väl inte tanka vad som helst i en bil? Du lär ta reda på att det är rätt bensin, diesel eller vad som kan tänkas behövas. Samma princip gäller för data. De digitala tjänster som byggs för högtryck behöver tillgång till rätt datamängder. Att avgöra vilka som är de rätta kräver datamognad, vilken stärks med arbete med klassificering av data.

Eric Hjelmestam

Roll: VD
Arbetsplats: MetaSolutions
Vårt/ mitt jobb: Att få arbeta med ökad öppenhet och samtidigt digitalisera offentlig sektor är anledningen att vi jobbar på MetaSolutions gör dagligen. För alla som börjar arbeta med data/ informationshantering/ informationssäkerhetsfrågor så är säker delning av data var en central.

Tankar kring informationssäkerhet i allmänhet och Teams i synnerlighet

Microsoft Teams en mardröm ur ett informationsstyrningsperspektiv . Efter att länge ha upparbetat kunskap och kompetens för att säkerställa organisationers informationshantering slås allt detta sönder på några månader under 2020 – och det händer *globalt och utan eftertanke.*

När jag tänker på informationssäkerhet med de lärdomar jag har fått efter snart 30 års arbetslivserfarenhet inom informationshantering, har jag en något annorlunda syn på informationssäkerhet. När jag talar med personer som har huvudfokus på informationssäkerhet inom sin roll i olika organisationer har de väldigt ofta en rimlig helhetssyn gällande den så kallade CIA-triaden.

Så snart jag sedan rör mig inom själva verksamheterna förändras den synen radikalt inom dessa. Enligt min erfarenhet får de tre delar som kallas CIA-triaden (confidiitiality/konfidentialitet, integrity/riktighet, availability/tillgänglighet) inte samma tyngd eller fokus. Inom verksamheterna ligger fokus till nästan 100 % på en del av tre delarna – konfidentialitet.

Riktighet kan i vissa fall eller i vissa typer av verksamheter diskuteras och ses som ett hot eller en risk, medan tillgänglighet är den del av triaden som får minst uppmärksamhet. Jag skulle vilja hävda att inom de dagliga verksamheterna är det absolut vanligaste klagomålet gällande informationshanteringen att informationen inte kan hittas. Det är dock mycket få som utifrån detta faktum kommer till slutsatsen att det är en risk eller ett hot att information inte kan hittas – det ses främst som något besvärligt. Informationens konfidentialitet spelar då inte så stor roll. Om information inte är tillgänglig spelar det

”Så varför ta upp detta i samband med att vi talar om informationssäkerhet? För att ur ett informationsstyrningsperspektiv är Microsoft Teams en mardröm.”

ingen roll hur känslig den är eller om den är riktig eller inte.

Att bara ha fokus på konfidentialitet är lite som att sitta på en trebent pall som saknar två ben. Det blir väldigt jobbigt att hålla balansen om inte rent av omöjligt. Med ett starkt fokus på vem som ska få eller inte ska få se informationen glöms själva tillgången till informationen bort. Jag tror exempelvis att många känner igen att när du väl har gjort en sökning i en implementation av Sharepoint, eller motsvarande systemlösning, får ni flera träffar på ett dokument med samma namn, eller nästan samma namn. Det är i de fallen vanligtvis svårt att kunna bedöma vilket av dessa dokument som är den senaste versionen eller om de är arbetshandlingar respektive godkända/tillgängliggjorda handlingar. Hela den här problematiken har sin grund i bristande informationsstyrning.

Vi som arbetar med informationsstyrning, informationssäkerhet och långsiktig informationshantering har brottats med dessa frågor i många år utan att det på det stora hela har blivit bättre. Medan vi ägnat oss åt att brottas med de ”traditionella” utmaningarna som av vissa fortfarande ses som nya, har något väldigt omvälvande hänt. Jag skulle vilja säga att det är ett paradigmskifte i dess sanna mening. Drivkraften bakom paradigmskiftet var den pandemi som drog fram och som snabbt krävde nya lösningar. Lösningen blev det här fallet Microsoft Teams.

Att det var Teams som fick bli motorn beror till stora delar på slumpen. Vi blev tvingade att i så hög grad som möjligt arbeta hemifrån, och med den dominanta ställningen som Microsoft har var det helt enkelt lättast att börja använda det verktyg som organisationerna redan hade inbäddat i programsviten M365.

Microsofts tjänstebaserade programsvit M365 med Teams fick ett mycket stort och hastigt genomslag. Utan att egentligen sätta sig in i vad det innebär att använda Teams skapas snabbt så kallade teams och kanaler. I början ofta helt fritt utan strategi eller plan. Interna och externa möten började hållas. Det chattades, och chattar sparades ibland när något viktigt hade behandlats, det delades dokumentfiler och ibland spelades möten in och blev videofiler. Praktiskt och relativt smidigt.

Så varför ta upp detta i samband med att vi talar om informationssäkerhet? För att ur ett informationsstyrningsperspektiv är Microsoft Teams en mardröm. Efter att under många år upparbetat kunskap och kompetens kring hur information på bästa och säkraste sättet bör hanteras samt mer eller mindre systematiskt försökt att implementera dessa kunskaper för att säkerställa organisationers informationshantering slås allt detta sönder på några månader under 2020 och det händer *globalt.*

En av Teams stora fördelar är att det är enkelt och relativt smidigt att komma i gång med. En person startar ett team, bjuder in ett antal personer och skapar kanske också några kanaler inom teamet för att få ordning. Så vad är problemet? Här kommer några exempel.[1]

Var hanteras informationen – det beror på. Varje team som skapas får automatiskt ett eget "bibliotek" i Sharepoint. Om kanaler läggs till skapar dessa automatiskt underbibliotek i Sharepoint. Här kan informationshanteringen till vissa delar styras. Du kan till exempel skapa en direktlänk i Teams till Sharepoint-biblioteket. Du kan sedan ha ett arbetssätt som säger att alla dokument som delas ska ligga där. Då är väl den frågan löst? Nja … Om du sedan bokar ett möte i Teams via Outlook och under det mötet delar dokument, skriver en chatt som sparas eller spelar in mötet – då kommer det du sparar att läggas i din *personliga* OneDrive for business. Om du i stället bokar mötet via kalendern i teamet så läggs det som sparas i biblioteket. Stor skillnad! Detta blir desto mer allvarligt när en person slutar och den längsta tid dennes konto sparas i M365 är 90 dagar.

Vi har vissa handlingar med sekretess i teamet – det får ni inte, säger kanske verksamheten. Nu är det dock människor vi har att göra med och det är onekligen smidigt att dela information via teamet. Vi lägger då en behörighet så att endast vissa inom teamet kan få tillgång till informationen. Nix, samtliga medlemmar i ett team har tillgång till all information som hanteras i teamet (om det inte finns privata kanaler) och har dessutom behörighet att ändra, flytta och radera informationen.

Vi behöver dela det här styrande dokumentet mellan olika teams – det går inte. Om det behöver delas i flera teams måste dokumentet läggas till i varje team och läggs då in i respektive Sharepoint-bibliotek (om det inte delas i ett möte bokat i Outlook). Nu finns samma version av styrande dokument utspritt i ett okänt antal kopior och endast medlemmar i respektive team kan söka dokumentet, inte den centrala administratören av systemlösningen. Eventuellt kan denna göra en sökning via Sharepoint, men det är mer än vad jag vet.

Vad en central administratör vanligen kan se är antal teams, antal kanaler, vilka som är medlemmar i teamen, vilka som är ägare av teamen samt hur många gäster som finns i teamen. Det enda en organisation i bästa fall styr centralt är hur många teams respektive kanaler som får finnas i varje team, vilka som ska kunna skapa teams, hur många som får vara medlemmar i respektive team och så vidare. Varje team fungerar normalt, ur ett informationssäkerhetsperspektiv, som en helt isolerad silo. Det går att göra sökningar och det ska, enligt Microsoft, vara möjligt att exportera sökresultat men hur det ska gå till är i varje fall för mig lite luddigt. Framför allt undrar jag vad som menas med "exportera sökresultat"? Är det bara filerna eller kommer även metadata med?[2]

Dokumenthanteringsfunktionen är sekundär i Teams. Meddelandefunktionen är det primära syftet med Teams och den går inte att styra. Om du är medlem i ett team får du *alla* meddelanden vilket *gör* att medlemmarna tenderar att använda chatten mer, och inom vissa organisationer har chatten i Teams börjat ersätta intern e-post.

Det har nu påbörjats arbete med en slags retrospektiv styrning av Teams. Jag vill hävda att det arbetet kommer att i hög grad likna de försök till styrning av gruppdiskar med mappstrukturer som uppstod under 1990-talet och omkring 20 år framåt. Vi har nog alla, över viss ålder, varit med om när det ska "städas och ordnas" i de organiskt framvuxna mappsturkturerna på en gruppdisk och hur bra det brukade gå. Hur svårt det är att i efterhand försöka styra upp och besluta hur olika mappar ska användas och vilka informationstyper som ska ligga var. Det ska bli mycket intressant att följa arbetet med att få en styrning av verktyg som Teams och att se vilka konsekvenser användandet av dessa kommer att få för organisationerna. Jag ser också som arkivarie fram emot den dag en organisation säger: "Goddag, vi vill arkivera Teams." Förhoppningsvis har jag då gått i pension.

Källor

1. En brasklapp här. Utvecklingen av tjänsten Teams går oerhört snabbt och det är svårt att få en överblick om du inte har tid att följa med. Efter att det här har skrivits kan det mycket väl ha gjorts förändringar som gör att det som beskrivs här inte längre stämmer. Dessa förändringar sker hela tiden i bakgrunden och styrs helt av Microsoft.

2.Se https://learn.microsoft.com/sv-se/microsoft-365/compliance/ediscovery-?view=o365-worldwide

Leif "Peppe" Pettersson

Roll/yrke: Arkivarie
Arbetsplats: ArkivIT
Har arbetat som arkivarie i drygt 25 år och har genom åren haft fokus på informationshantering inom organisationer och hur vi använder informationen i vårt dagliga arbete. De senaste åren har Peppe främst arbetat med olika aspekter av digitalt bevarande.

6 snabba med Daniel Lilliehöök

Hej Daniel, vi börjar med en "enkel" fråga, varför är det viktigt för organisationer att ha en plan för arbetet med informationssäkerhet?

Informationssäkerhet är ett brett område som berör både personer, processer och teknik. För många organisationer är det svårt att veta vad som är viktigast, eller vilken ände man ska börja i. Risken blir då att man antingen fokuserar på fel saker, eller kanske inte gör något alls. En plan baserad på branschens best practice är en stor hjälp att komma i gång i rätt ände och börja göra bra saker!

Vari ligger riskerna att inte ha kontroll över sin informationshantering?

Många associerar informationssäkerhet främst med hotet att illasinnade hackers ska komma över känslig eller hemlig information. Vilket så klart kan vara en reell risk. Men faktum är att större delen av informationssäkerhetsincidenter handlar om interna misstag som till exempel kan leda till att viktig information blir fel, eller inte går att komma åt när den behövs. Detta kan ge stora effekter och kostsamma avbrott i verksamheten. Därför är det viktigt att ta ett helhetsgrepp över sin informationshantering, och tänka på säkerheten i alla de tre perspektiven Konfidentialitet, Riktighet och Tillgänglighet.

Har och i så fall hur din roll som enterprisearkitekt inverkat på det arbete du bedriver inom området informationssäkerhet?

Som enterprisearkitekt upplevde jag ibland att säkerhet betraktades som "någon annans problem", och som något som man kan lägga till i efterhand. På samma sätt kan jag uppleva att informationssäkerhet ibland tenderar att bli en lite för "isolerad ö" som skriver policys och dokument som inte på riktigt hjälper utvecklare och förvaltare att faktiskt höja sin säkerhet. Samtidigt handlar både informationssäkerhet och enterprisearkitektur till mångt och mycket om samma saker! Båda berör ämnen som processer, information, IT-system, hårdvara, fysiska lokaler, och leverantörer. Så det finns en väldigt stor synergi att få dessa två discipliner att samarbeta närmare med varandra!

Vad är cybersäkerhet och är det en del av informationssäkerhetsarbetet?

Cybersäkerhet har blivit ett populärt ord som används för nästan allt som har med informations- eller IT-säkerhet att göra. Traditionellt så

"Men faktum är att större delen av informationssäkerhetsincidenter handlar om interna misstag som till exempel kan leda till att viktig information blir fel, eller inte går att komma åt när den behövs."

tolkar jag det som att cybersäkerhet är den del av teknisk IT-säkerhet som har med externa hotkällor att göra. Teknisk IT-säkerhet i sin tur är en del i det mer övergripande begreppet informationssäkerhet, som också inkluderar administrativa säkerhetsåtgärder.

Berätta lite mer om den programvara ni utvecklat på Omegapoint och vad den hjälper kunderna med

När vi började utveckla vårt verktyg så var ambitionen att bygga en plattform där både arkitekter och informationssäkerhetsexperter skulle arbeta tillsammans i ett och samma verktyg. Det har med tiden blivit en relativt komplex produkt som fungerar både som ett översiktligt arkitekturmodelleringsverktyg och ett stödsystem för informationssäkerhetsarbete. Vi kallar det numera Compliance and Information Security Organizer, eller ”Ciso” i korthet.

Och slutligen, om man står handfallen och inte vet var man ska börja- vilka är dina bästa tips och lärdomar från dina år i branschen?

Ta hjälp av de standarder och best practices som finns! Tex.ex. strukturera arbetet och organisationen kring informationssäkerhet i enlighet med ISO 27001. Och så klart – undvik att jobba med alltför många Excellistor och lösa dokument, och använd i stället ett bra verktyg där ni kan samla allt och både få en överblick, borra ned i detaljer, och bygga upp en historik för hur ert informationssäkerhetsarbete utvecklas över tiden!

Daniel Lilliehöök

Roll/yrke: Ph.D., Enterprisearkitekt och informationssäkerhetsexpert

Arbetsplats: Omegapoint

Daniel har en bakgrund som IT- och enterprisearkitekt, och jobbar sen ca 7 år inom gränslandet mellan arkitektur och informationssäkerhet. Daniel är en av grundarna av bolaget Innovate Security och har varit drivande av utvecklingen av det egna stödverktyget för informationssäkerhet och modellering som idag heter Omegapoint Ciso (tidigare ESM). Läs gärna mer om det på ciso.se!

’En it- arkitekts perspektiv på informationssäkerhet och molntjänster’

Hur gör vi när vi vill ta hem information från en molntjänst på ett säkert sätt. Denna artikel beskriver ett sätt som utifrån it-arkitektur kan stötta verksamheten på ett övergripande sätt

Molntjänster innebär för många verksamheter en smidig tillgång till applikationer, information samt problemfri drift, men det kan också innebära utmaningar. Hemtagning av information på ett säkert sätt är ett sådant exempel. Ett sätt att adressera detta är en strategi kring en helhetsvy från IT-arkitektur och som kan ingå i utforskande och agila arbetssätt. Denna strategi syftar till att skapa förutsättningarna för alla de roller som behövs för att säkerställa information och informationshantering, direkt genom roller som säkerhetsspecialister men även andra roller som beställare, användare från verksamheten, tjänstedesigners och roller inom projektledning och test.

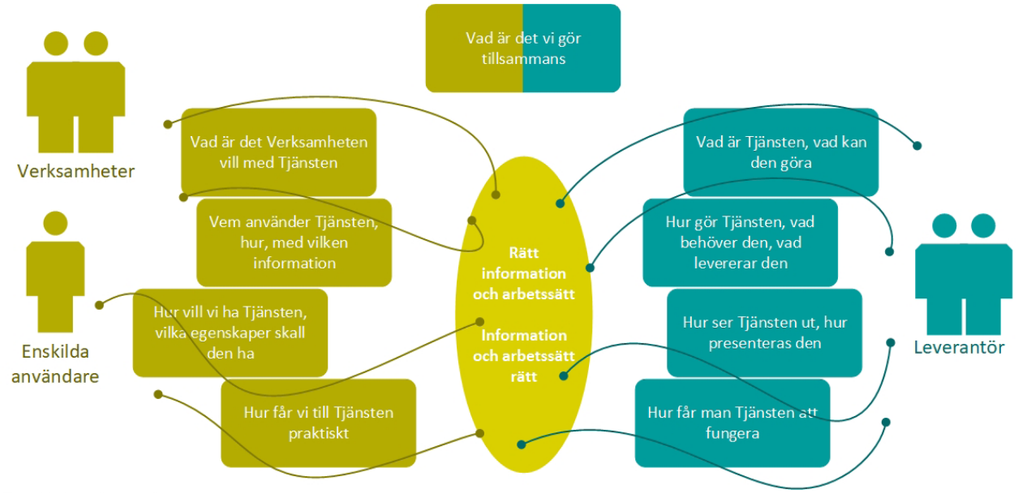
Vid en första anblick kan det verka enkelt att ta hem sin information på ett säkert sätt. Vi vet ju vilken information som finns i tjänsten. Vi vet hur säkerheten ser ut kring förbindelse och åtkomst till informationen. Eller vet vi det? Vet vi vad som döljer sig bakom de funktioner molntjänsten erbjuder? Vet vi hur den är uppbyggd och hur informationen egentligen hanteras? Och framför allt, vet vi egentligen hur vi själva faktiskt använder den och hur verksamheten ser ut på vår sida?

Ett helhetsperspektiv på hur en verksamhet använder en molntjänst
Detta är en generell modell av en produkt eller molntjänst utifrån verksamhetens eller kundens perspektiv, och som även visar olika nivåer på kundens verksamhet och hur dessa motsvaras av vad tjänsten erbjuder. Detta helhetsperspektiv är grunden för att skapa förståelse för hur digitalisering går till och vad det är verksamheten behöver. Perspektivet från en kund är också viktigt eftersom det är så tjänsten uppfattas utifrån.

Vad är det vi gör tillsammans? Detta handlar om syfte och mål med tjänsten och vad verksamheten vill ha ut av den. Detta kan ofta hämtas från ett projektdirektiv eller annat måldokument och exempelvis vara att verksamheten behöver en molntjänst för att lagra arbetsdokument och där tjänsten erbjuder ett smidigt sätt att jobba, säkerhet i form av tillgänglighet, backup och problemfri drift. Om vi antar att scenariot att ta hem sin information handlar om en molntjänst för dokumentlagring, behöver man börja redan här och beskriva syftet med att informationen skall tas hem. Det kan vara förändrad driftsform eller en lokal backup. Utifrån det kan man börja förstå vad det innebär att ta hem informationen.

Vad är det verksamheten vill med tjänsten? Detta är en första detaljering för att förstå både vilken information tjänsten egentligen har, och hur den används, så att vi alltså vet både vad det är vi behöver ta hem och hur vi kan fortsätta använda informationen. I exemplet med molnlagring av dokument kan verksamhetens behov vara möjlighet att lägga upp, hämta, ändra dokument, men också samarbeta kring dokument, dela ut dokument till olika användare och kanske kunna arbeta med dokumenten direkt i molntjänsten. Man brukar benämna detta förmågor

Vad är tjänsten och vad kan den göra? Motsvarar nivån som ovan beskrivits, men för tjänsten. Här måste vi börja i vad det är vi vill ha innan vi kan tolka vad tjänsten erbjuder och vad det innebär. Men sedan måste vi även se vad tjänsten erbjuder för förmågor som vi kanske inte tänkt på, eller var medvetna om att vår verksamhet faktiskt använde. Vi börjar här också få en bild över de stora dragen kring hur information lagras och flyttas, grundläggande perspektiv för den mera tekniska säkerheten, men även för det säkerhetsmässiga perspektivet. Med detta avses den mera tekniska säkerheten men eftersom säkerhet börjar med hur information används, att den alltså kan användas på samma sätt efter att den hämtats hem och används lokalt eller migrerats till en ny tjänst.



En arkitekturell översikt

Vem använder tjänsten, hur, med vilken information? Detta är en detaljering som utgår från användarna, vilka roller de har och vad de gör, mera detaljerat. Här ingår processperspektivet med aktiviteter och mera detaljerade beskrivningar av informationen, det som löser förmågorna vi hittade i tidigare nivåer. Det viktiga är att inte gå in på lösningar och teknik utan hålla sig på nivån kring användare som utför aktiviteter och vilka leverabler i form av dokument och annan information som produceras och förändras. En viktig aspekt här är att även verksamheten har mål och syften. Detta är lika viktigt att fånga som användarnas perspektiv

Hur gör tjänsten'? är motsvarande nivå för tjänsten, och även här är det bra att utgå från verksamhetens sätt att göra saker, men även vad tjänsten erbjuder för funktioner som vi kanske inte var medvetna om, till exempel versionshantering kanske finns i en dokumentlagrings-tjänst och som verksamheten först inte var medvetna om men visar sig vara användbar. Det säkerhetsmässiga perspektivet fortsätter här att utvecklas genom de grundläggande insikterna om vad det faktiskt är vi skall säkerställa; att verksamheten kan fortsätta arbeta, kanske inte på samma sätt, men med samma resultat, vad användare och verksamhet vill uppnå och vi måste förstå hur saker görs för att veta att vi hämtar hem all information vi behöver och att vi kan arbeta med den på samma sätt. Vi får också en mera detaljerad bild kring vad tjänsten innehåller för information, var den finns och hur den flyttas

Hur vill vi ha tjänsten, vilka egenskaper skall den ha? samt Hur ser tjänsten ut, hur presenteras den? Gällande egenskaper så börjar vi närma oss it-lösningar och i viss mån teknik. Detta brukar också kallas 'icke-funktionella krav'. Att börja med vad verksamheten behöver är viktigt men det är ofta så att man även tittar på vad tjänsten erbjuder. Egenskaper som skalbarhet för ökade krav på prestanda både vad gäller volym, antal användare och responstider är sådant som har säkerhetsmässig betydelse framför allt vid en migrering, för att användare ska kunna fortsätta hantera informationen. Kanske inte direkt säkerhetsmässigt kopplat, men en aspekt är kostnad som dessa egenskaper ofta är förknippade med. Är det lösbart om vi flyttar vår information. Mera direkt säkerhetsmässigt är en förståelse av redundans, backup och att tjänsten är tillgänglig. Detta är ofta något man behöver förstå praktiskt tillsammans med leverantören.

Andra egenskaper som är viktiga är "Leverantör"'. Vad erbjuds för support? Var finns leverantören eller underleverantörer? Detta är viktigt säkerhetsmässigt utifrån dataskyddslagstiftning men även praktiskt. Vi behöver veta var vår information egentligen finns, både geografiskt men även om informationen är samlad eller om informationen är samlad inom molntjänsten alternativt lagras eller hämtas från andra tjänster. Detta berör återigen underleverantör men även tredjeparts- tjänster och vad dessa gör. Mera tekniska aspekter här rör driftmiljö: Hur är redundans och backup utformad? Var finns alternativa datacenter och vad händer vid driftstörningar? Hur länge kan tjänsten vara nere innan ett backupsystem tar över? Riskerar vi att tappa information i dessa lägen? Även aspekter som hur ofta back-up utförs och vad som kan gå förlorat mellan dessa behöver has i åtanke. Det finns även egenskaper utifrån användbarhet som behöver beaktas. Är tjänsten och hur verksamheten tillämpar den förståeligt och hur får vi med förståelsen vid en migrering så att informationen säkras mot felhantering? En sista egenskap att titta på rör integrering med andra system vi använder. I exemplet med en dokumenthanteringstjänst hur hantering av dokument hänger ihop och risker när vi lämnar en tjänst utifrån både teknisk kompabilitet och sätt att använda tjänsten.

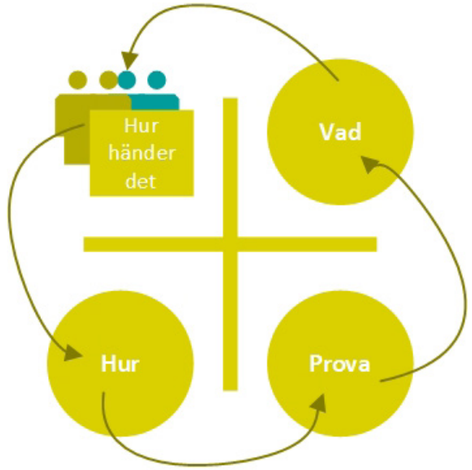
Hur får vi till tjänsten praktiskt? och Hur får man tjänsten att fungera? Dessa frågor rör lösningar och teknik. Detta avslutar egentligen det vi började med högst upp. Det vill säga att tjänsten ska kunna realisera verksamhetens syfte och vision med den, den ska erbjuda användarna vad de vill ha och de egenskaper de behöver Allt detta skall realiseras med det som tjänsten erbjuder. På denna nivå finns tekniska specifikationer som operativsystem, kommunikations-protokoll, filformat och beskrivningar av informationsobjekten. Detta är viktigt både för att säkert kunna ta hem sin information och för att informationen ska vara förståelig och användbar för verksamheten eller vid migrering till en ny tjänst. Det är också viktigt för att uppskatta storlek och kapacitet, både hos leverantör, i förbindelse och hos verksamheten när det gäller att ta hem stora mängder, eller komplexa strukturer, av information.

I ett sammanhang

Den modell av en tjänst och hur den används som beskrivs här är generell, men i det här sammanhanget rör det informationssäkerhet. Modellen visar därför hur säkerhet inte bara handlar om information och hur den lagras och överförs eller teknisk implementation, utan även om vad användare behöver samt hur verksamheten säkras utifrån olika situationer som kan uppkomma kring livscykeln när man använder en molntjänst .

Detta arbete befinner sig också i ett sammanhang där det finns en beställare och med projektledning. Arbetssättet passar bra in i agila former men fungerar även i mera traditionella, linjära projekt. Att adressera en helhet i nivåer stöttar också i att ta fram underlag för planering och riskbedömning, särskilt scenariobaserad sådan som ofta utgår från vad användare gör.

Beskrivningen i denna artikel ligger på en strategisk nivå. Hur man sedan utför de olika delarna praktiskt, analyserar, beskriver, verifierar, beror på typ av arbete och hur man gör i den verksamhet där man arbetar. Framför allt också utifrån de roller som finns i verksamheten, arkitekter, tjänstedesigners och kompetenser inom säkerhet och systemutveckling. En bra fortsättning för att få sådant här arbete på plats är att hämta inspiration ifrån utforskande arbetssätt från design-rörelsen, som också utgår från syfte och behov och hela tiden provar slutsatser



Om man vill veta mer kring att bedriva arbetet enligt utforskande och ansatsdrivna arbetssätt så beskrivs det bra i böckerna "Lean UX" av Josh Gothelf och Josh Seiden och "Continous discovery habits " av Teresa Torres. Flera bra verktyg finns i metodiken "Design sprint ", ursprungligen framtagen av Jake Knapp,och från SKR "Innovations-guiden.se".

För att stärka samarbete kan den övergripande modellen skrivas ut och hängas på en vägg, whiteboard eller liknande och där kan man fästa Post-It:s, anteckna, rita eller skriva ut modeller för att driva arbetet. Digitala verktyg som fungerar bra med detta sätt att arbeta och visualisera är t.ex. Visio, Miro, Milanote och Draw.io.

Detta arbetssätt beskrivs och utvecklas av artikelförfattaren, mera specifikt för informationsförvaltning, på siten www.informationsforvaltning.com och för Design av Digitala Produkter, på siten www.attt.se som författaren driver. På dessa webbplatser finns fördjupningar kring metodik och nedladdningsbara modeller i olika format.

Verktyg och resurser
Verktyg och resurser finns i stor omfattning och det som erfarenhetsmässigt fungerar och som brukar användas inom IT-arkitekturarbete är förmågebaserad kartläggning, process- och informationsmodeller. Dessa använder ofta formella modellspråk, exempelvis Archimate. På nivåerna kring lösning används ofta informations-, integrations- och lösningsmodeller för att detaljera. För egenskaper kan man söka på färdiga listor för "system quality attributes", hos b.la Wikipedia. Resurser inom IT-arkitektur finns hos svenska www.iasa.se samt Iasa International iasaglobal.org.

Mats Andréasen

Roll: Verksamhetsarkitekt

Arbetsplats: Göteborgs stad

IT-arkitekt med erfarenhet från offentlig förvaltning och industri b.la telekom och medicintekniska produkter. Engagerad i information och dokumentförvaltning genom uppdrag i Näringslivets Arkivråd. Också engagerad i att etablera IT-arkitektur, designtänkande och agila metodiker genom engagemang i Sveriges IT-arkitekter och olika Meetup-forum.

IT-säkerhet handlar inte om teknik

Det finns studier som pekar på att 97 procent av alla IT-attacker riktar in sig på att lura användare med någon typ av cyber-psykologi.[1] Bara det borde väl räcka som argument för att vi ska sluta se IT-säkerhet som en fråga om teknik, när det i själva verket handlar om oss människor. Om vår förmåga att stanna upp, tänka efter, fråga och rapportera när vi upptäcker något som verkar misstänkt. För lärande är inte ett event. Det är en process.

Att antalet cyberattacker fortsätter att öka kommer nog inte som någon överraskning. Den som följer nyhetsrapporteringen kan regelbundet se nyheter om allvarliga dataintrång hos både företag, organisationer och offentliga aktörer. Ingen går säker.

Den digitala sårbarheten har dessutom ökat till följd av distansarbetet under pandemin. 2021 ökade antalet attacker med 21 procent – en större ökning än under de fem föregående åren sammanlagt.[2] Det verkar som om cyberattackerna nu lagt sig på en konstant högre nivå. Prognoser från Europeiska unionens cybersäkerhetsbyrå (Enisa) pekar på att alla typer av samhällsviktiga organisationer kommer att behöva satsa mer på cybersäkerheten som en del av digitaliseringen.[3]

Den kanske viktigaste siffran för att förstå vad cyberattacker beror på, och hur vi ska skydda oss mot dem, är denna: Cyberkriminella lyckas fortfarande ta sig in i nätverken hos över 9 av 10 företag. Och studier visar att 9 av 10 lyckade attacker börjar med bristande säkerhetsförståelse hos enskilda medarbetare.[4] Därför måste alla organisationer prioritera och stärka sina mänskliga brandväggar.

IT-säkerhet funkar inte om inte alla medarbetare är medvetna om säkerhetsriskerna – fråga IT-experterna! Enkäter visar att hela 87 procent av säkerhets- och IT-experter håller med om att det helt enkelt inte går att bygga upp en fungerande IT-säkerhet utan att samtidigt utbilda all personal.[5] Därför behöver alla typer av organisationer prioritera sina mänskliga brandväggar lika mycket som sina tekniska och satsa lika mycket på utbildningen av sin personal som på tekniska investeringar. Det är även viktigt att inte heller lämna över IT-säkerheten endast till säkerhetsexperterna.

Att skapa en stark säkerhetskultur – i hela organisationen – är det bästa sättet att förebygga mänskliga misstag. Studier visar att regelbundna och effektiva utbildningar skapar en kultur där anställda bättre förstår sin del i organisationens säkerhetsarbete. Frågan är bara: Hur går man tillväga??

Organisationens IT-mognad avgör

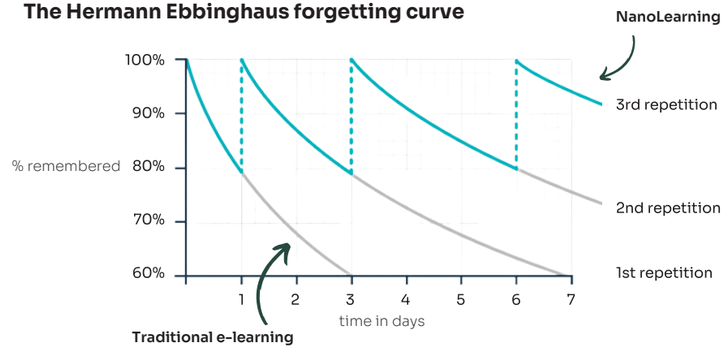
Att inse att en fråga är strategisk är en sak. Att veta hur man hanterar den långsiktigt är en annan. Och här finns inga ”quick fixes” att ta till. Att stärka informationssäkerheten handlar i grund och botten om att skapa en fungerande säkerhetskultur byggd på öppenhet.

De flesta organisationer går igenom ett antal utvecklingsfaser i sitt säkerhetsarbete:

1. Förnekande
Många organisationer befinner sig fortfarande i en typ av förnekelse, en inställning om att ”så länge inget händer så behöver vi inte göra någonting”.

2. Reaktivt
Alltför många företag och organisationer inser att informationssäkerhet är viktigt – först när olyckan har inträffat. Incidenter leder alltid till aktivitet. Men det reaktiva förhållningssättet räcker inte.

3. Systematiskt
Vi ser att allt fler organisationer har informationssäkerheten som en del av sina ledningssystem. Här har ISO27001 (om krav på informationssäkerhet) spelat en starkt pådrivande roll.



4. Proaktivt
När säkerhetstänket börjar bli en del av organisationens utvecklingsarbete så har man kommit en bra bit på väg. Säkerhet som läggs till i efterhand blir aldrig bra. Säkerhet som tänks in redan när nya system och arbetssätt sätts upp får en mycket bättre effekt.

5. En del av vardagen
Först när informationssäkerheten är en del av alla medarbetares vardag, när IT-säkerheten ”sitter i ryggmärgen”, kan man säga att en säkerhetskultur med möjlighet att påverka säkerhetsnivån i företaget på ett positivt sätt finns på plats.

För att en organisation skall ha en möjlighet att ta de här stegen och skapa en fungerande säkerhetskultur, krävs också en öppenhetskultur. En organisationskultur som gör att alla medarbetare känner sig uppmuntrade att dela med sig av fel och misstag – även sådana de själva har gjort – och där den som rapporterar misstänkta fel och brister blir belönad, inte kritiserad och ifrågasatt.

”Därför behöver alla typer av organisationer prioritera sina mänskliga brandväggar lika mycket som sina tekniska och satsa lika mycket på utbildningen av sin personal som på tekniska investeringar.”

Stort mörkertal

Även om vi ständigt möts av rapporter om det ökade antalet cyberattacker, så är mörkertalet fortfarande stort. De flesta organisationer som blir utsatta för till exempel ransomware väljer att inte kommunicera detta, i ett försök att skydda sitt varumärke. Det finns studier som pekar på att bara 10 procent av alla cyberattacker verkligen rapporteras.[6]

Det är ett stort misstag. Flera exempel de senaste åren visar att organisationer som varit öppna med vad som drabbat dem tvärtom

har stärkt sina varumärken. Såväl Coop som Kalix kommun och Norsk hydro har alla vunnit uppskattning och respekt för sitt sätt att kommunicera vad de varit med om. Deras arbete har även tjänat som ett riktmärke för andra att ta efter. Öppenhetskulturen behövs både inom och mellan organisationer samt inom branscher och över sektorsgränser. Utan en gemensam öppenhetskultur kommer vi som arbetar för ökad informationssäkerhet aldrig att ha en chans mot cyberkriminella – som ju hela tiden delar med sig av kunskap och erfarenhet i en hisnande fart.

Beteendeförändrande lärande är nyckeln

Nyckeln till framgång är att sluta se lärande och utbildning som event och börja se lärande som en process. Redan på 1880-talet beskrev Hermann Ebbinghaus den så kallade glömskekurvan och sedan dess har vi människor fortsatt att glömma bort nästan allt vi lär oss.[7]

Det vill säga: om vi inte får chansen att repetera och reflektera.

Många organisationer strävar efter att bli lärande organisationer och att skapa ett *”learning mindset”*. Det är helt rätt tänkt – även när det gäller cybersäkerheten. De som lyckas med detta är de som i grunden klarar av att ställa om från event till process och som hittar fungerande metoder som både klarar av att vinna kalenderkriget och får med alla på tåget. Som ser till att designa sitt lärande enligt grundmetoderna *spaced*[8] och *retreval*[9]. Som ger kunskapen tid att sjunka in och deltagarna en möjlighet att använda förvärvad kunskap i praktiken.

Att skapa en fungerande säkerhetskultur handlar alltså inte om teknik utan om oss människor och vårt lärande. Och minst lika mycket om att lära om, som att lära nytt. Invanda beteenden och vanor sitter i och tar lång tid att förändra. Att se lärandet som en process och inte som ett event är den enda chansen att klara den förändringen.

Källor

1. 2022 Global Cybersecurity Awareness Training Study (ThriveDX)

2. Verizon 2022 Data Breach Investigations Report

3. https://www.enisa.europa.eu/news/cybersecurity-investments-in-the-eu-is-the-money-enough-to-meet-the-new-cybersecurity-standards

4. 2022 Global Cybersecurity Awareness Training Study (ThriveDX)

5. 2022 Global Cybersecurity Awareness Training Study (ThriveDX)

6 IMY, rapport 2022:1, Anmälda personuppgiftsincidenter 2021 MSB, Cybersäkerhet i Sverige 2021 – i skuggan av en pandemi

7. https://en.wikipedia.org/wiki/Forgetting_curve

8. https://en.wikipedia.org/wiki/Spaced_repetition

9. https://www.retrievalpractice.org/why-it-works

Per Lagerström

Roll/yrke: Kommunikationsansvarig

Arbetsplats: Junglemap – ett företag som med hjälp av NanoLearning hjälper företag att bygga mänskliga brandväggar året runt.

Att skydda och hantera företagets information i agila utvecklingsprocesser.

Hur skyddar och beaktar man informationen i systemen när företaget arbetar med egenutveckling av system? Många bolag arbetar idag med så kallade agila processer. I artikeln skall jag försöka belysa de utmaningar som finns och som behöver hanteras beträffande it och informationssäkerhetsarbetet när man arbetar på detta sätt.

En process har en början och ett slut. Varje process har oftast flera aktiviteter. Det är så vi är vana vid att arbeta. Under ett antal år nu har det agila arbetssättet blivit populärt. Men vad innebär det egentligen och på vilket sätt kan det påverka arbetssättet och resultatet ur ett it- och informationssäkerhetsperspektiv?

Säkerhet måste finnas med från början. Men många säkerhetsmoment kanske inte alltid kommer med tidigt i ”projektet”. Man måste fokusera på vissa typer av frågor. – Vad är syftet med systemet? Vilken typ av information skall hanteras och vilka krav är kopplade till informationen? Enklast att förstå detta är genom informationsklassning, där möts krav och skyddsbehov tydligare. Hur ser processerna ut? Vilka förmågor finns tillgängliga eller vilka nya skapas? Titta på arkitekturen, flöden, känsligheten på informationen, alltid tillsammans med verksamheten. D.v.s. utvecklare, informationsägare, scrum master, systemägare etc. Var finns brister eller risker?

Bakgrund

Agila processer har väl egentligen inte riktigt någon början eller något slut, men aktiviteterna i utvecklingsarbetet kan ha en början och ett slut. Det man i första hand tänker på är förändring eller förbättring, eller om man så vill ständig förändring och förbättring av en tjänst, ofta utifrån en kodbas (programkoden) som förändras och förhoppningsvis förbättras.

Med denna förbättring bör, gärna i steg i den agila processen som testning, arkitekturfrågor, säkerhetsfrågor och datahantering vara givna i denna kontinuerliga process av utveckling, förbättring och förändring. Men hur ser det egentligen ut?

Det finns några agila arbetssätt och det finns några ramverk att ta till sig som stöd i detta sätt att arbeta. Jag kommer dock inte att gå in på dessa, utan bara fokusera på utmaningarna med agilt arbete i utvecklingsprocessen generellt.

Det som oftast existerar i organisationer är att man tagit några grundläggande tankar och gjort om det till sin egen agila process. Detta kan i sig, i viss mån, göra det till en utmaning när man kommer till säkerhet och kvalitet. Min erfarenhet är att man inte alltid får med alla viktiga delar som kan behövas, saker rinner ut i sanden eller förloras helt utifrån vad som kommer ut från det agila arbetet eller ”processen”.

Säkerhet och kvalitetsbrister

Erfarenheten från flera företag pekar på just det ovanstående. Man tar lite av varje från olika modeller och gör det till en agil process. Man tar gärna med sig att gruppen, teamet, som arbetar med utveckling också måste ta hand om vissa viktigare delar i underhållet, tex drift. Det tydligast i denna tanke är uttrycket ”You build it, you run it”. Även ansvarsfördelningen kan vara en sådan sak som gärna tas till teamet och det landar oftast i att det blir ett gemensamt ansvar. Det är här som man kan börja se utmaningar i den utvecklingskod som kommer ut . Det blir inget tydligt ansvar. Oftast leder det till brister i kvalitet, säkerhet och uppföljning, något som kan påverka backlog (typ av restlista) tydligt och göra att den växer. Det i sin tur kan skapa en teknisk skuld , (i detta fall fel i kod eller kod som bör åtgärdas) Nästa fråga är vem som hanterar icke funktionella krav? Dessa krav har ofta koppling till lagkrav, företagets säkerhetspolicy m.m.

Mycket av grundtanken med agilt arbetssätt är att individer har ett starkt intresse i det de arbetar med och att man har ett starkt samarbete där man tar ett gemensamt ansvar för att få leveransen att fungera. Det är en fin tanke med entusiastiska medarbetare, men

fungerar den i verkligheten?
Tyvärr verkar den inte alltid göra det. Ska man generalisera lite så är ofta utvecklare endast intresserade av att just utveckla. Alla krav och delar av leveransen som inte har med utveckling att göra kan hamna lite vid sidan om, ramla mellan stolarna, glöms bort eller ignoreras, exempelvis effektivare driftfrågor eller icke funktionella krav. Man kan se DevOps och DevSecOps roller som något bristfälliga i många team. Företagen kan ha väldigt genomtänkta team, men oftast är det främst utvecklare med fokus på kodutveckling, inte på drift eller icke funktionella krav samt andra delar eller ansvar. Ett exempel är detta med drift ”24/7” som inte alltid blir som det är tänkt, om inte teamet organiserat samarbetet ordentligt samt haft en tydlig ansvarsfördelning och uttalade förväntningar. Här ser vi återigen vikten av ansvarsfördelningen. Vem tar vilken roll och när? Ska det vara flera i den rollen som är ambulerande? Icke funktionella krav kan också vara något som missas. Det är av vikt att någon i organisationen belyser de krav som finns och hjälper teamen att få med dessa, gärna i samarbete med till exempel en produktchef/produktägare. Men detta sker inte alltid, då affären vill ha fokus på just affären, vilket gör att grundläggande drift och säkerhetsfunktioner inte prioriteras vilket återigen kan skapa teknisk skuld eller backlog som kan bli svårt att hantera då den oftast växer sig stor och komplex.

Det är en del frågor som måste beaktas, annars kan det sluta med att man får en halvfärdig produkt som ser bra ut på ytan, men som i själva verket är en stor teknisk och informationssäkerhetsrisk vid leverans, på grund av just brister på säkerhet, som också då påverkar kvaliteten på leveransen. Här har vi ytterligare en möjlighet, eller utmaning (många ser säkerhet som ett arbete som är i vägen), nämligen riskarbetet. Har vi en bild på risker som kommit upp? Hur ser riskerna ut för hela organisationen eller för vissa team? Information som kan vara till stöd i det strategiska arbetet i organisationen. Kanske behöver vi fokusera på viss typ av utbildning i delar av utvecklingen eller vissa team? Proaktivitet är ledordet.

Helhetsbilden – Komplexitet och säkerhet hör inte ihop!

En annan risk som jag uppmärksammat är den komplexitet som skapas när flera grupper uppfinner hjulet på nytt, de olika teamen samarbetar inte. Missar man samarbetet och kommunikationen skapas en ”overhead” på teknikval. Med det menas ett onödigt arbete med olika plattformar och förmågor som gör samma sak. Detta påverkar arkitekturstyrning på många sätt, som i sin tur påverkar datakvalitet och kontroll. I slutändan blir då helhetsbilden inte som vi tänkt oss.
Vi har en del risker och vi har en del onödig komplexitet som leder till att vi får säkerhetsproblem samt störningar och leveransproblem av it. Detta kommer även innebära onödiga kostnader, som kanske inte syns, men som påverkar marginalen på affären i slutändan. Många bäckar små skapar en dyr it drift…

Lösningen är nära till hands?!

Hur löser man detta? Det finns nog inte ett tydligt svar på detta, bara idéer. Men det finns knep att ta till. Till exempel att arbeta med nedanstående lista. Listan är utan inbördes ordning. Det finns garanterat mera knep, diskutera i din organisation vad som brister i ert arbete.

Se till att:

• Ansvar finns och är tydligt i de olika teamen och rollerna. Vem ska man prata med när så behövs för olika typer av funktion, krav eller fundering?

• Styra funktionskraven, designkraven och säkerhetskraven på ett strukturerat sätt.

• Arbeta över alla team med arkitektur och förmågor samt verktyg och funktion.

• Ta hjälp av olika tekniker såsom kodgranskning, tester, standarder för kodhantering, gemensam kodbas med information om kodkvalitet, funktion och kontroll/test av kod t.ex. ISO 27034.

• Informationssäker och bra testdata finns. Det finns flera organisationer som kan bistå, till exempel så har Skatteverket fejkade data med personnummer.

• Arbeta med ett flexibelt riskhanteringsverktyg.

• Ledningen förstår vilka krav som bör ställas och vem som har ansvar för vad. Delat ansvar är ingens ansvar. Ledningen måste förstå, översiktligt, hur man får fram kvalitet i sitt utvecklingsarbete och vad som krävs. Informera, håll dem uppdaterade och utbilda!

• Organisera team så de inte fastnar eller missar viktiga grundkrav eller leveranser och ansvar.

• Köra PI-planning/Big room planning för att synka, dela kunskap och insikt samt arkitekturförståelse.

• Teamen har insikt om vad som förväntas av dem.

• Produktägare, scrum master m.fl. har ett gemensamt forum, gärna tillsammans med arkitektur och CTO, där de utbyter koderfarenhet, teknikval och process, arbetssätt samt arkitektur och förmågor, samt fokuserar på samma mål!

Nedanstående bild ger en inblick i när man kan fokusera på vad och vid rätt tidpunkt:

Sebastian Nisser Blanck

Arbetsplats: Spectrem AB

Driver sedan december 2021 eget som Java-utvecklare med säkerhetsfokus. Jag är en van utbildare och har varit talare på bla Omegapoints kompetenskonferens, Certezzas säkerhetsdag och DataTjej, m.fl.

Under mina uppdrag har jag lagt ett stort fokus på CI/CD, samt att bedriva SecDevOps, både inom teamet och för hela organisationen.

Jag älskar nya utmaningar och att jobba lösningsorienterat, därför har jag erfarenhet av att agera projektledare, scrum-master, arkitekt och mentor när det har behövts.

Kent Illemann

Roll: Egenföretagare på illemann konsult AB

Kent Illemann har arbetat brett inom olika delar av IT i cirka 30 år, de senaste 15 åren med huvudfokus på IT & Informationssäkerhet. Idag arbetar Kent som egenföretagare på illemann konsult AB inom säkerhetsområdet och har hjälpt kunder och företag såsom bland andra Trygg Hansa, Ericsson, Com Hem, Tre, Tieto Evry och Praktikertjänst, men även kommuner samt statliga bolag att effektivisera och utveckla sin IT-och informationssäkerhet. Kent är också en uppskattad lärare och föreläsare inom området och sitter i styrelsen för SIG Security.

Den nya vardagen

Ni har alla sett bilden i tidningar och TV under rubriken Hacker: en mörk siluett med luvtröja som sitter framför en dator. Bilden är kraftigt missvisande och borde i stället vara en bild från ett datacenter med rader av kraftfulla datorer. Det är ingen människa som letar efter just din organisation; maskiner söker runt på nätet för att ta sig in via era brister och sårbarheter. Ibland lyckas dom. Var och varannan dag kan vi läsa om välfungerande bolag som fått in ransomware (utpressningsprogram) och behövs stoppa hela eller delar av sin verksamhet, trots att de har en IT-säkerhetsavdelning och mängder av avancerade skydd. På IT-säkerhetsslang säger man ”att dom blev ägda”. Vad gjorde dom för fel? Vad har ni för chans att klara er?

Den dåliga nyheten är att om en stark aktör, t.ex. en stat, bestämmer sig för att ta er, så klarar dom det. Då gäller det att ha ransomware-säkra backuper och vältränade processer. Den goda nyheten är att ni kan skydda er så att ni blir svåra att ”äga” - det är inte komplicerat, bara jobbigt att bli ”ett hårt mål”. Denna artikel kommer hjälpa er på vägen.

Överblick över IT-säkerhet
Som ledare för att förbättra IT-säkerhet behöver du inte alla detaljer, men du behöver överblick så du kan styra arbetet. Denna överblick kan ges med följande bild.

Execution (Genomförande)
Det operativa arbetet består i att Skydda era system och information, Reagera i tid när något händer, Hantera det som sker och Planera för att bli bättre på att Skydda, Reagera och Hantera.

Objectives (Mål)
Målet vi ska uppnå med informations- och it-säkerhet är

• Confidentiality (Konfidentialitet): Skyddsvärd data ska hållas oåtkomligt för icke-betrodda. Ingen ska kunna sno dina lösenord eller ta sig in på ditt LinkedIn-konto.

• Integrity (Riktighet): Informationen ska vara korrekt. Ingen ska kunna manipulera er information.

• Availablity (Tillgänglighet): Informationen ska vara nåbart, när ni behöver den. I dagligt tal pratar vi ofta om säkerhet och stabilitet, men faktum är att hålla systemen vid liv och få tillbaka dem efter en crash eller ransomware är en del av it-säkerhetsarbetet.

• Overview (Översikt): Utan överblick kan du inte veta att du är säker. Om du har ett kontor med hundratals dörrar behöver du en panel för att se att alla är låsta. Bland de organisationer vi träffar är oftast Överblick det största problemet, inte minst i molnet. Bolag idag har många system och att snabbt få upp nya gör att man snabbt kan tappa överblicken.

Tools (Verktyg)
Human 1 (Människan): Det första, och viktigast verktyget är människor – era anställda och konsulter. En vis man sade en gång: ”Människor, lösningen på, och orsaken till, alla it-säkerhetsproblem”. Ni måste få medarbetarna med er och se till att de får tid att får bort ”smutsen”.

Human 2 (Verktyg för människan): Människans arbetsminne klarar bara att hålla 7 +/- 2 saker i huvudet – 5 om vi är stressade och 9 om vi är helt fokuserade. En bra minneshjälp är ramverk som OWASP, ISO 27001, CIST och liknande. Dessa är inte en lösning på problemen utan bara verktyg för att strukturera arbetet.
Technical (Tekniska): Lösenordshanterare, brandväggar, virusskydd och liknande ökar skyddet.

Physical (Fysiska hjälpmedel): Om någon har fysisk access (och tid) till din laptop eller era servrar så kan man ta sig in. Passerkontroller, larm, kassaskåp, digitala nycklar skyddade i speciell hårdvara är alla exempel på fysiskt skydd.

Legal (Juridik): Ett bra avtal kan göra att du kan minska andra skydd. Inom vården så kan personal läsa en journal för en patient de vårdar. Men om någon läser en journal för en patient de inte vårdar så riskerar de böter eller att bli av med arbetet.

Enablers (Möjliggörare)

Det börjar med ledarskap.
Hur ska ni som organisationen strukturera er för att klara utmaningarna?

Hoten mot svenska organisationer är större än någonsin. De som vill bryta sig in är välorganiserade och rika. Idag är malware-marknaden (speciella skadeprogram) specialiserad. Några är bäst på att ta sin igenom det yttre skyddet, och sedan säljer de ingången till de som är bättre på att ta sig vidare, något som på engelska kallas Lateral Movement. Brister finns alltid i alla organisationer. Det är lätt att råka ställa in något fel i brandväggen eller glömt att man tillfälligt stängde av virusskyddet. Nya sårbarheter upptäcks varje vecka. Det är ett evighetsjobb att hålla saker uppdaterade så att inte sårbarheterna läggs på hög. Hur ska man hinna med? Konsekvenser av bristande IT-säkerhet läser vi om i pressen och på Twitter. Ena dagen står kassorna på Coop stilla, den andra så står Maersks containrar stilla då logistiken har fallerat. A-kassorna kan inte betala ut pengar till några av de mest behövande i samhället, och deras problem drar med sig andra bolag i fallet för datacentret de använde inte hade separerat kunderna tillräckligt. Hur ska vi bygga en organisation som klarar av att hantera riskerna från **Hot, Brister, Sårbarheter-Konsekvenser?**

Igen, det börjar med ledarskap. Någon måste bestämma vilken av riskerna man vill ta, då det inte finns någon väg framåt som är riskfri. De tre viktigaste sidorna av problemet är följande:

• Affären: De som tjänar pengar när systemet är i gång.

• Juridik: De som ska skydda organisationen mot legala risker.

• IT-säkerhet: De som ska skydda organisationen mot IT-risker.
Se dessa delar som sittande i var sitt hörn av en triangel och de drar åt olika håll. It-säkerhet vill ha allt supersäkerhet så det knappt går att jobba. Juridik tycker att vi helt ska undvika att använda persondata, fast då kan vi inte sälja eller skicka varor. Affären vill tjäna pengar och röra sig fortare framåt än konkurrenterna. Någon måste bestämma var i triangeln ”man sätter krysset” – vilken balans man vill ha av de tre olika viljorna. Svaret är enkelt: Affären sätter krysset. Det är de som tjänar pengar på att systemen är i gång och ledsna om de går ner. Jobbet för juridik och it-säkerhet är att förklara på vardagligt språk vad olika val innehåller för Hot, Brister, Sårbarheter - Konsekvenser. Bäst är om man kan få ner valen till två: Ska vi uppdatera systemet omedelbart och få bort sårbarheten, men riskera en minskad försäljning, eller ska vi ta risken att ha kvar sårbarheten några dagar till och uppdatera på natten mellan lördag och söndag? Ni som är hemma med RACI-matrisen: Affären är Responsible, medan jurdik och it-säkerhet är Consulted. Affären tar risken och andra delar av verksamheten lyfter fram Hot, Brister, Sårbarheter-Konsekvenser så Affären kan välja risk

Vad brukar det finnas för motstånd i en organisation att börja hantera risker på ovan sätt? Oftast är det kulturen – det finns ett motstånd mot att lyfta information och IT-säkerhetsproblem. Det är inte så konstigt: Du sitter och jobbar som vanligt och försöker hinna med allt och klara budget. Plötsligt får du veta att golvet affären står på är ruttet och kan rasa när som helst. För många är den omedelbara psykologiska reaktionen att slå bort det – problemet är komplext, och konsekvenserna är obehagliga. Tyvärr är det alltför vanligt att problemen mörkas och budbären tystas ner. Det finns en logik i det. Nya problem stör planeringen. Du kanske inte har budget för det. Att berätta för din chef att något i din avdelning är trasigt kan mötas med bistra kommentarer, eller t.o.m. repressalier. Å andra sidan finns det alltid en katastroffond

Om en ”olycka” händer så kan man kasta in hur mycket personal och konsulter som helst. Löser du och dom incidenten snabbt så kan ni få applåder. Då ingen förutsåg det så var det ingens fel. Så titta inte efter. Vänd inga stenar. Lyft inte upp problem.

Hur vänder man då en negativ kultur till en som ser positivt på att lyfta fram saker som behöver fixas? Man måste börja högst upp. Vi konsulter har en viktig uppgift att fylla i att förklara till ledingen att hot är det nya normala, samt att brister och sårbarheter finns överallt. Information och it-säkerhet är komplext, men att beta av synliggjorda problem är mest jobbigt. Om ledarskapet visar uppskattning på hittade problem och ger beröm ifall det presenteras förslag på hur man löser det, så förändras kulturen snabbt. Det kommer att finnas motstånd på grund av obehaget för konsekvenserna varför medarbetare måste ges utrymme att lufta och diskutera. I förändringsarbetet så kan det vara bra att ta in en konsult på heltid. Hen kommer in med andra ögon, och kan som någon som står utanför rådande kultur bli den som lyfter de tunga frågorna. I andra fall finns det saker som talar emot att sikta på att få in en info/it-säkerhetskonsult på heltid.

1. Det är stor brist på kunniga personer.
2. Det nya normala är att behöva skydda sig – nu och i framtiden.
3. Info/IT-säkerhet ska vara en naturlig del i de anställdes arbete.
4. Det operativa, vad man behöver göra, går att googla sig till eller med AI som bollplank.
5. 2-head policy. På alla viktiga delar bör organisationen ha minst två personer som kan det.

Kort sagt, er organisation måste bli självgående. Så om vi bortser från förändringsarbetet, är ofta bästa lösningen att ha en konsult på timmar som kommer in då-och-då och hjälper till med det taktiska och strategiska. I vilken ordning är det lämpligt att göra saker? Vad behövs för kompetenser? Var står vi nu och vad är gapet till dit vi vill komma? Hur vet du om konsulten är bra? Ovan gick vi igenom hur viktigt det är att i vardagligt språk förklara Hot, Brister, Sårbarheter - Konsekvenser. Så förstår du vad konsulten pratar om så är sannolikheten hög att den är värd sitt pris.

En snabbkurs i info/IT-säkerhet

Du kan inte skydda det du inte vet du har

Vilka system har du, vad gör de och vad innehåller de för data? Om du kan svara säkert på frågan ovan, så har du lagt grunden för info/IT-säkerhetsabetet. Du behöver inte gå en fyraårig utbildning för att få det hela på plats – du behöver ”bara” kommunicera med medarbetare och leverantörer. Jobbet är tungt och tar tid, men livet blir mycket lättare när det är gjort – både vad gäller GDPR och it-säkerhet. Vill du ha guldstjärna så ser du till att teknikerna tar fram bilder på hur alla system prata med varandra. Vilka system anropar vilka? Vilka portar används?

Det finns bara tre sätt att ta sig in

Många konsulter och leverantörer pratar om sina fantastiska lösningar. Hur man kan köpa sig fri bara man lägger pengarna hos dem.- För att bättre förstå om du verkligen behöver deras erbjudande är det bra att veta på vilka sätt man tar sig in i system:

- Något är trasigt
- De använder dina rättigheter
- Du bjuder in dem

Trasigt är saker som fel i mjukvara, felkonfigureringar m.m. Har de kommit över dina lösenord, så kan de göra samma saker som du får göra. Klickar du på en länk eller installerar ”smutsig” programvara så har du bjudit in ovälkomna gäster i ditt hus. I många fall kommer de in via en kombination av ovanstående tre punkter. Ett exempel är att någon klickar på en länk och ”smutsig” programvara kan installeras för att operativsystemet inte är uppdaterat och innehåller kända hål.
För att minska risken så är det grundläggande att ha ordning och reda:

- Håll alltid allt du har uppdaterat
- Validera dina konfigurationer
- Se till att ingen har mer rättigheter än de behöver för att utföra sitt jobb
- Använd starka lösenord som är unika för varje tjänst.
- Lagra dina lösenord så det är endast lättåtkomliga för dig med en lösenordshanterare
- Slå på multifaktorautenticering (MFA)
- Ha phishing-skydd på din mejlserver
- Skydda dina klientdatorer och servar med Endpoint Detection and Response
- Centralisera dina användaridentiteter och slå på de extra skydd som moderna lösningar erbjuder

Anamma Zero Trust

Det finns lika många förklaringar på vad Zero Trust (ZT) är som det finns tjänster och system att köpa. IT-marknadens aktörer har starkt hoppat på detta modeord och kan visa upp många grafer och bilder, den ena mer komplicerad än den andra. I själva verket är det enkelt.

ZT = Onion + PoLP2

Onion (Lökprincipen): Du ska ha så många lager, så hårda som möjligt. Bygg inte en kokosnöt – ett hårt skal på utsidan, men mjukt på insidan. Ditt jobb är att hitta vilka lager du kan addera.

PoLP 1: Principle of Least Privilege – ingen medarbetare eller systemkonto ska ha mer rättigheter än de behöver för att göra sitt jobb.

PoLP 2: Principle of Least People – du ska inte ha fler personer än du behöver som har höga rättigheter.

Sköt din medarbetarprocess (X-boarding)

Om medarbetare inte har de rättigheter som de behöver så hör de av sig – om de byter tjänst internt eller slutar och har kvar rättigheter så hör man inte någonting.
Bygg upp en process för att hantera stegen från att de signerat kontraktet till de inte lägre jobbar kvar (På engelska X-boarding – X:et har nedan ersatts med prefix):

- Pre-boarding: när personen skrivit på avtalet så kan man ge dem rätt att läsa mejl och kurser.
- On-boarding: vid start av anställningen eller uppdraget så bör medarbetaren ha allt som behövs för att jobba.
- Cross-boarding: ta bort rättigheter som inte behövs längre när någon byter tjänst.
- Off-boarding: Se till att blocka allt så snart någon slutar. Centraliserat rättighetssystem är till stor hjälp – låser du användaren är allt klart.

I teorin är det enkelt med PoLP och X-boarding, men i praktiken är det ett stort jobb att få överblick över alla system och dess inbyggda rättigheter. Inte komplicerat, men jobbigt. När man gjort det tunga lyftet och få till det, så måste det kontinuerligt upprätthållas, då både organisation och system förändras.

Skaffa er ransomware-skyddade backuper genom ”air-gapped vault”

Lägg era backuper på ett ställe som ingen som har rättigheter till den vanliga miljön har tillgång till. Om någon tar över hela er miljö så har de inte någon möjlighet att hoppa över till den separata miljön. Det går enkelt att lösa med ett separat konto i molnet som t.ex. några i styrelsen som inte jobbar operativt har inloggning till. Backuperna synkar man sedan upp med skript som så ofta som man behöver.

Risker och ramverk

Som du noterat har vi ovan pratat mycket om Hot, Brist, Sårbarhet och dess Konsekvenser – de delar som skapar en risk. Samtidigt så kanske du känner till att det pratas om att man ska jobba på ett ”risk-baserat arbetssätt”. För att gå till botten med frågan, behöver vi börja med att definiera vad risk är. Wikpedia definierar det såhär: “In simple terms, risk is the [possibility] of something bad happening.” Grunden är alltså sannolikhet. Det är tyvärr vanligt att man i dagligt tal kallar hot, brister och sårbarheter för risker. Några exempel:

- ”Anonymous Sudan är en stor risk”. Denna attackgrupp är ett hot.
- ”Våra system har en risk då de inte är uppdaterade”. Systemen har sårbarheter.
- ”Vi har en risk i våra avtal då vi inte har med en GDPR-klausul”. Avtalen har brister.

Vi människor kan inte uppskatta risk – sannolikheten att något dåligt händer. Det är för vi har inget inbyggt system för att i hjärnan att ”mäta” det. Ett exempel: Det finns människor som är rädda för att flyga – det mest säkra transportsätt vi har. Samtidigt kan dessa personer utan att bli nervösa köra många km/h för fort trötta i en bil till flygplatsen för att sedan stressade springa över vägen om de håller på att missa flyget. Vad gäller IT-säkerhet så är det inte vi som har ägandeskapet om risken – det är den som attackerar. I vissa fall kan vi mäta risker: I repetitiva system. Flyg är ett sådan system. Överallt händer samma sak: man taxar, startar, stiger, får kaffe när man är upp på höjd, sjunker, landar och taxar igen. Samlar vi alla gånger något dåligt händer så får vi ett medelvärde på risken. Dock är it-säkerhet inte repetitivt – hela idén med en attack är att den ska vara ovanlig – då är det större sannolikhet är det att den lyckas. Om vi nu inte kan uppskatta risker eller mäta den, så kan vi med bestämdhet säga att vi inte ska tillbringa tid att gissa risker.

Så hur ska vi jobba riskbaserat? Det finns en sak som vi vet om risk: vi vill att den ska bli mindre! Om vi motverkar Hot, tar bort Brister och Sårbarheter så minskar risken för att Konsekvensen infaller.

Att jobba riskbaserat betyder att strukturerat och kontinuerlig ta bort ”smuts”. Har ni en organisation som hittar ”smuts” så är det bara att lägga in vad som behöver göras i ett ärendehanteringssystem – desto fler hittad ”smuts”, desto bättre är organisationen på att identifiera risker. Mät sedan även på hur många ärenden som är gjorda och redovisa per kvartal eller halvår. En annan trevlig konsekvens av att mäta på antalet hittad och borttagen är att när det börjar bli ”rent” inom ett område så är det svårare att hitta saker att ta bort. Så börjar de leta extra noga. Det är precis det du vill!

Hur får du upp er lista med vad som behöver fixas? TTH – Talk To Humans. De som jobbar “på golvet” vet alla saker som behöver fixas – det är bara att fråga dem och sedan ge dem tid och resurser att fixa. Nu vet vi att när man börjar prata om det så blir listan snabbt lång. En dags session med en bra konsult kan ge månader av jobb.
Hur prioriterar man? Det är enkelt: Fråga personen närmast problemet hur stor smärta det är att saken inte är lagad. Sätt ett värde från 0 till 100. Be dem sedan att uppskatta hur jobbigt det är att lösa saken. Fråga inte hur många timmar det tar! Ställer vi den frågan så tänker folk på när de jobbar (som bäst) och glömmer lätt strul, möten, problem med att få tag på rätt information m.m. Nu har vi två mätvärden att använda för prioritering: Smärta och Jobbighet. Tänk dig ett diagram med Smärta på Y-axeln och Jobbighet på X-axeln. Du kan t.o.m. sätta upp notis-lappar med det du ska göra på en whiteboard med ritade X- och Y-axlar. Prioritering: Lös först de sakerna med mycket Smärta och lite Jobbighet, sedan de med medel Smärta och Jobbighet osv. Du kanske aldrig hinner med de med låg Smärta och hög Jobbighet. Det är OK, för vi vet vad som är viktigare.

Ramverk och certifiering

Nu några ord om ramverk som avslutning. ISO 27001 fokuserar på processer. Man kan jämföra det med hur restaurangen är på att hantera recept. Du blir inte en bra kock på att hantera recept – du blir bra av att kontinuerligt laga mat. Gå ut i köket och laga mat! Få saker gjort. Recepten kan du skriva sen. Vi kan även använda liknelsen för att bedöma konsulter: Du kan inte fejka att laga mat. Samma gäller för it-säkerhet. Se till att hålla borta de konsulter som bara kan prata recept. Ta hjälp av de konsulter som kan stå i köket med er och laga mat.

Lars Morre Mårelius

Roll: VD Tentixo

Hjälper organisationer med att bygga IT-säkerhet, global infrastruktur och utveckla stabil mjukvara.

Micke ”Lex” Lexelius

Roll: VD och grundare av Lex Security AB

Bakgrund från Försvarsmakten inom informations- och säkerhetsarenan och myndigheter inom Total Försvaret.
Tidigare ledamot inom SACS (Swedish Association of Civil Security). Säkrar samhällskritisk och känslig information tillsammans med kund när han inte är ute och fiskar eller åker skidor med sina barn.

Främja säkerhetsmedvetenhet i den digitala eran:

Utmaningar och lösningar för kunskapsförmedling och praktisk tillämpning

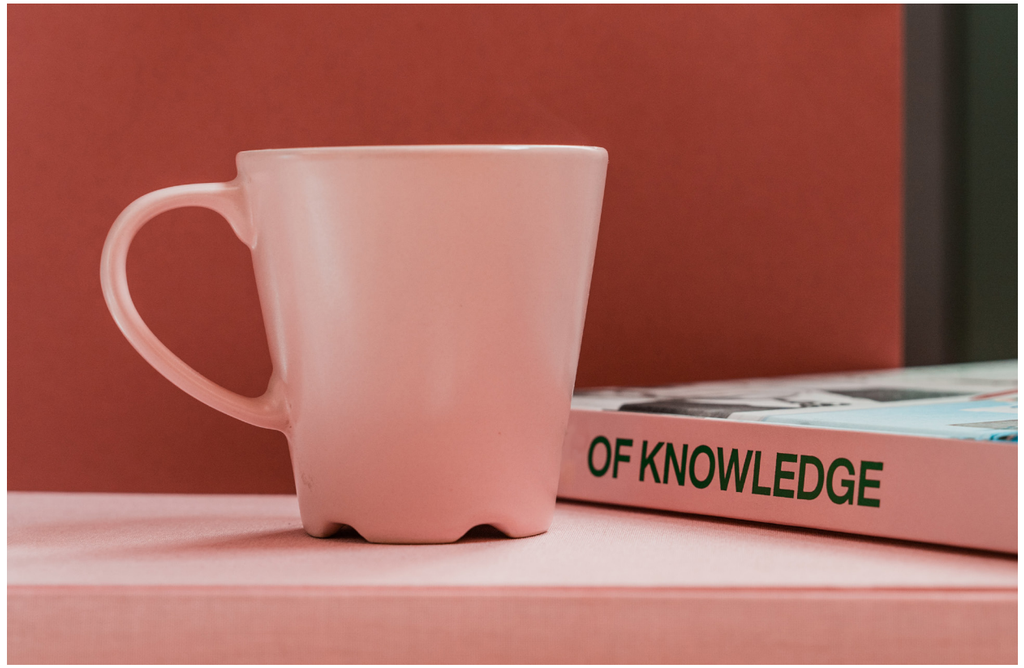
Denna artikel tar upp utmaningarna med att lära ut och främja säkerhetsmedvetenhet i dagens digitala värld. Genom att använda online-kurser och simulerade cyberattacker, strävar vi efter att göra användare medvetna om deras roll inom cybersäkerhet. Artikeln belyser fem kärnutmaningar: kunskapsförmedling, bibehållande av kunskap, praktisk tillämpning, kundrelationeroch användarrelationer – och hur vi på IT-säkerhetsföretaget Nimblr hanterar dem.

Vi är lärande individer, födda med förmågan att lära av egna och andras erfarenheter. Vi har lärt oss allt vi kan, nästan allt vi gör samt hur vi ska förstå och interagera med vår omvärld. Trots vår inlärningsförmåga är det inte alltid helt okomplicerat att lära ut. Även om lärandet kan vara både belönande och motiverande, måste kunskap förmedlas på ett sätt som möter inlärningen. Vårt uppdrag på Nimblr är att lära ut säkerhetsmedvetenhet (Security Awareness, SA) till våra användare via online-kurser och simulerade cyberangrepp. Många cybersäkerhetsincidenter uppstår på grund av användarnas misstag och brist på kunskap, och det är därför mycket viktigt att hjälpa användare att förstå deras betydelse när det gäller cybersäkerhet. Ett effektivt utbildningsprogram i SA stärker användarnas medvetenhet om de säkerhetsrisker som deras beteenden kan medföra, och belyser misstag som användare ofta begår, till exempel när de hanterar e-post, surfar på internet eller hanterar hårdvara. Att konstruera en effektiv SA-tjänst fordrar betydligt mer än att bara rada upp instruktioner systematiskt. Här följer fem specifika utmaningar förknippade med förmedlandet av säkerhetsmedvetenhet, samt beskrivningar av vårt förhållningssätt och hanteringsstrategier när det gäller dessa utmaningar.

Den första utmaningen: Kunskapsförmedling

Online-lärande har gjort det möjligt att övervinna begränsningar beträffande tid och plats, men fordrar hög motivation hos deltagarna på grund av den begränsade sociala interaktionen. Motivationsfrågan är särskilt relevant för den sortens SA-utbildning som vi bedriver, där kunderna beställer en utbildning som deras anställda, slutanvändarna, sedan förväntas genomföra. Inlärningen sker således inte på självvald basis, utan utgör ett extra arbetsmoment för användarna. Det är därför förståeligt att användare uppfattar utbildningen som en sekundär, lågprioriterad uppgift. Eftersom framgången med SA i hög grad beror på hur väl användarna accepterar utbildningsverktyget är vår utmaning att öka deras engagemang och att göra utbildningen relevant, intressant och tidseffektiv. Här får vi inte glömma det primära uppdraget, vilket är att ge användarna lämplig och relevant kunskap för att möjliggöra en beteendejustering i säkerhetsmedveten riktning. Läromålet är således ett processmål snarare än ett examensmål. En viss nivå av baskunskaper är nödvändig. Om användaren exempelvis inte vet att Microsoft inte aktivt ringer upp användare för att tala om att deras dator är infekterad av virus är det mycket troligare att användaren uppfattar samtalet som legitimt. När tillräcklig kunskapsnivå är uppnådd blir dock vaksamhet och träning viktigare än faktakunskaper.

Vi har hittills valt att inrikta kursinnehållet på vad alla inom organisationen behöver känna till. Vi har noterat att användare är mindre benägna att ta till sig kunskap från ett SA-program om de överväldigas av för mycket information och om programmet kräver en stor tidsinvestering. Detta kan istället resultera i minskad motivation att lära sig och mindre effektiv kunskapsbehållning. Utbildningen ska således aldrig ta mer tid i anspråk än nödvändigt – vanligtvis mindre än en halvtimme per månad – och undvika informationsöverbelastning. Vidare strävar vi efter att hålla en konstruktiv och stödjande ton och göra inlärningen intressant och levande med hjälp av verkliga exempel, illustrationer och humor.



Andra utmaningen: Bibehållande av kunskap

Säkerhetsmedvetenhet är inte resultatet av en enstaka träningsinsats, utan en kontinuerlig process som strävar efter att öka användarnas medvetenhet om risker, hot och hur deras individuella handlingar kan påverka organisationens totala riskexponering. Av central betydelse för denna process är att användare bibehåller sin kunskap över tid samt att kunskapen uppdateras i takt med den snabba teknologiska utvecklingen. På Nimblr bemöter vi denna pedagogiska utmaning främst genom s.k. “spaced repetition”, en inlärningsteknik som innebär att användarnas tidigare kunskaper friskas upp med jämna mellanrum.

Tredje utmaningen: Görandet

Detta hänger ihop med den förra utmaningen. Säkerhetsmedvetenhet är inte någonting vi har, utan något vi gör. Säkerhetskunskap saknar värde om det inte leder till att användare förstår vikten av informationssäkerhet, är medvetna om potentiella hot och motiverade att lära sig och implementera rätt säkerhetsbeteenden. Användare behöver förstå varför SA är viktigt, både för den egna och för organisationens säkerhet, samt träna in säkerhetsfrämjande rutiner med utgångspunkt i den egna organisationskontexten. SA-utbildningen behöver således integreras i den dagliga verksamheten. Vi är måna om att utbildningen utformas på ett sätt som tillåter den att löpa parallellt med användarens normala arbetsuppgifter. De simulerade angrepp som vi erbjuder som primära träningsredskap är anpassade efter kundspecifika variabler, och följs upp med feedback och påminnelser. Genom att göra utbildningen personligt relevant och integrerad i användarens verklighet vill vi främja ett tillväxtinriktat tankesätt, där deltagarna upplever att deras förmågor utvecklas genom övning och där misstag ses som inlärningsmöjligheter.

Fjärde utmaningen: Kundkontakten

För att användaren ska kunna se sina misstag som lärotillfällen fordras att organisationen har samma inställning. När säkerhetsmisstag leder till utpekanden och bestraffningar blir säkerhetskulturen lidande.

”Av central betydelse för denna process är att användare bibehåller sin kunskap över tid samt att kunskapen uppdateras i takt med den snabba teknologiska utvecklingen”

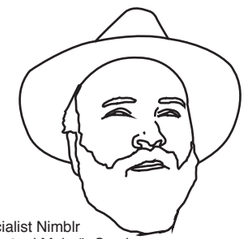
I en sådan arbetsmiljö försöker användare hemlighålla sina klavertramp vilket ofta leder till att incidenter och säkerhetsbrister åtgärdas för sent. Misslyckanden bör självfallet inte eftersträvas för sin egen skull, men kan ge värdefulla insikter, främja problemigenkänning, uppmuntra organisatorisk flexibilitet och erbjuda erfarenhet för att hantera problem i framtiden. En organisations förmåga att etablera ett klimat som främjar lärande och stödjer individuell utveckling är av enorm betydelse för en SA-utbildnings effektivitet. Här begränsas vår roll till att ge användare och kunder den kunskap och beredskap som behövs för att skydda sig själva från säkerhetsmisstag och cyberangrepp. Framgången med säkerhetsmedvetenhet beror i hög grad på hur väl kunden accepterar verktygen. Ibland kan organisationer betrakta utbildning som en kostnad snarare än en investering. En sådan inställning leder till att de endast uppfyller minimikraven för utbildning, vilket inte är tillräckligt för att skapa en stark säkerhetskultur. Chefer spelar en avgörande roll i detta sammanhang. De behöver inte bara förmedla effektiva och engagerande budskap om cybersäkerhet, utan också föregå med gott exempel.

Femte utmaningen: Användarrelationerna

Ett effektivt och framgångsrikt ramverk för SA online levererar inte bara innehåll, utan fokuserar även på att skapa en positiv, stödjande och engagerande inlärningsmiljö, där deltagarna är i centrum för sin egen inlärning. Inom traditionellt e-lärande poängteras ofta vikten av att både användare och utbildare uppfattas som ”riktiga personer” i medierad kommunikation, men i fallet SA-utbildning är detta mer komplicerat. Som tidigare nämnts har våra användare blivit ålagda att genomgå utbildningen av sina arbetsgivare, våra kunder. Relationen mellan oss och våra användare bör således genomsyras av

lyhördhet och respekt för användarnas integritet. Vi behöver måna om sekretess och personuppgiftsskydd; vi profilerar inte våra användare i onödan och samlar inte heller in mer användarinformation än absolut nödvändigt för att kunna erbjuda interaktiva kurser och simuleringar. På samma gång som vi diagnosticerar organisationens säkerhetsberedskap och rapporterar om användarnas kursdeltagande och säkerhetsefterlevnad strävar vi efter att föra en transparant dialog med användarna om vad som rapporteras och varför.

Sammanfattningsvis är SA en cyklisk process av medvetenhet, träning och utbildning på både individuell och organisatorisk nivå, och uppdraget att lära ut säkerhetsmedvetenhet innebär specifika och lärorika utmaningar när det kommer till alla dessa faktorer. Detta är vår läroprocess. Vi är, när allt kommer omkring, lärande individer, och lärandet fortsätter.



Martin Karlqvist

Online Behavioural Specialist Nimblr
Jobbar från vårt huvudkontor i Malmö, Sverige
martin.karlqvist@nimblr.se

Jonas Hedbäck

Account manager Nimblr
Jobbar från vårt säljkontor i Lissabon, Portugal
jonas.hedback@nimblr.se

Källor

Al-Fraihat, Dimah, Joy, Mike, Masa'deh, Ra'ed & Sinclair, Jane. Evaluating e-learning systems success: An empirical study. Computers in human behavior. Vol. 102, 2020: 67–86. https://doi.org/10.1016/j.chb.2019.08.004

Alotaibi, M., & Alfehaid, W. (2019, March 10-13). Information security awareness: A review of methods, challenges and solutions [Conference paper]. Internet Technology and Secured Transactions, London, UK. 2019.

Ananga, Patricia. Pedagogical considerations of e-learning in education for development in the face of COVID-19. International Journal of Technology in Education and Science (IJTES). Vol. 4, 2020: 310-321.

Guimaraes, Johnny (2021). Information security awareness: Learning for effectiveness. 2021.

Kumar, Vikas & Sharma, Deepika. E-learning theories, components, and cloud computing-based learning platforms. International Journal of Web-Based Learning and Teaching Technologies. Vol. 16, 2021: 1-16.

Skärpta regler om informationssäkerhet för handlingar som rör Sveriges säkerhet

Hantering av och skydd för elektronisk information ges stor uppmärksamhet. Det är inte konstigt med tanke på samhällets beroende av it, digitaliseringen och ständigt pågående angrepp där elektronisk information görs otillgänglig eller kommer på avvägar. Men information på papper kan vara minst lika viktig att ha kontroll över – i synnerhet när det handlar om Sveriges säkerhet.

Om säkerhetsskyddsklassificerade uppgifter röjs för obehöriga skadas Sveriges säkerhet. Sådana uppgifter ska enligt säkerhetsskyddslagen skyddas mot bland annat spionerier. Det handlar inte endast om informationssäkerhet utan även om fysisk säkerhet och om att personer som i sitt arbete hanterar uppgifterna är pålitliga och har kunskap om säkerhetsskydd.

Den 1 januari 2023 skärptes reglerna inom det civila området för fysiska handlingar som innehåller säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass konfidentiell och högre. Tidigare gällde reglerna om exemplarhantering för säkerhetsskyddsklass hemlig. De skärpta reglerna träffar statliga myndigheter, regioner och kommuner men också företag som bedriver verksamhet som är av betydelse för Sveriges säkerhet. Anledningen till skärpningen är att Säkerhetspolisens regler har anpassats till försvarsområdets regler för att skapa ett mer nationellt enhetligt skydd för säkerhetsskyddsklassificerade uppgifter i exempelvis totalförsvarsplaneringen.

Reglerna om hantering av fysiska säkerhetsskyddsklassificerade handlingar finns främst i Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd men även i säkerhetsskyddsförordningen (2021:955).

”Behovet av säkerhetsskydd upphör inte när en säkerhetsskyddsklassificerad handling har arkiverats – det är fortfarande en säkerhetsskyddsklassificerad handling”

Från upprättande till förstöring – en säkerhetsskyddsklassificerad handlings livscykel

Hantering av en handling i säkerhetsskyddsklass konfidentiell eller högre kan beskrivas som en livscykel med åtgärder (se figur). Det ska finnas dokumenterade rutiner för åtgärderna. Åtgärderna säkerställer att den egna organisationen har kontroll över samtliga fysiska exemplar från det att handlingen kommer in eller upprättas till dess att handlingen har förstörts eller arkiverats.

För att upprätthålla kontroll över fysiska handlingar i säkerhetsskyddsklass konfidentiell och högre ska det finnas ett register över vilka fysiska handlingar som finns i den egna verksamheten. Registret är centralt för informationssäkerheten eftersom registret gör det möjligt att inventera handlingarna och säkerställa att alla handlingar har lämnats tillbaka när personal avslutar sin anställning. Registret behövs även vid utredningar om brott mot Sveriges säkerhet, t.ex. för att ta reda på vilka handlingar som en viss person har haft tillgång till.

Normalt hanteras de fysiska handlingarna och registret över handlingarna av en central funktion i verksamheten, vanligtvis en registratur eller annan funktion för dokumenthantering. En nyhet är att registret över säkerhetsskyddsklassificerade handlingar kan vara skilt från diarier över allmänna handlingar. Ett skäl för detta är att säkerhetsskyddsklassificerade handlingar inte endast förekommer hos myndigheter utan även hos företag. Även hos myndigheter kan

det vara lämpligt att använda ett diarium för ärendehantering och offentlighetsinsyn, och ett annat register för uppföljning av handlingar i säkerhetsskyddsklass konfidentiell eller högre.

Att ha kontroll över varje exemplar av en handling, bl.a. genom kvittering vid mottagande, inventering och dokumenterad förstöring brukar benämnas *exemplarhantering*. Varje fysiskt exemplar förses med ett nummer som identifierar exemplaret av en viss handling. Ett vanligt sätt är att det första exemplaret får exemplarnummer 1, det andra exemplaret *exemplarnummer 2* och så vidare. Kombinationen av *handlingens beteckning* och *exemplarnummer* identifierar unikt varje fysiskt exemplar.

Förutom att registret behöver innehålla uppgifter om varje handling, såsom dess rubrik och beteckning, ska registret även innehålla uppgifter om vem som har tagit emot exemplaret, när exemplaret inventerades och om exemplaret har återlämnats, arkiverats eller förstörts eller om det har förkommit.

Kvittering ger spårbarhet

En viktig åtgärd för att ha kontroll över de enskilda exemplaren är att mottagaren kvitterar att hen tagit emot ett exemplar. Det finns några olika sätt att ordna kvittenserna, där ett sätt är att kvitteringen görs med underskrift på ett kvitto. Kvittot innehåller uppgifter om vilket exemplar som tas emot, vem som tar emot det och när det togs emot.

Årlig inventering bidrar till ordning och reda

En kontroll av att varje exemplar av en handling är i behåll ska göras minst en gång per år. Underlag för kontrollen hämtas från registret och resultatet antecknas också i registret. Om ett exemplar konstateras vara saknat, indikerar det en säkerhetshotande händelse. Vissa händelser, bland annat otillåtna röjanden, ska anmälas till Säkerhetspolisen. Den årliga kontrollen bidrar också till ordning och reda bland exemplaren, eftersom de ska kunna visas upp.

Återlämning och förstöring

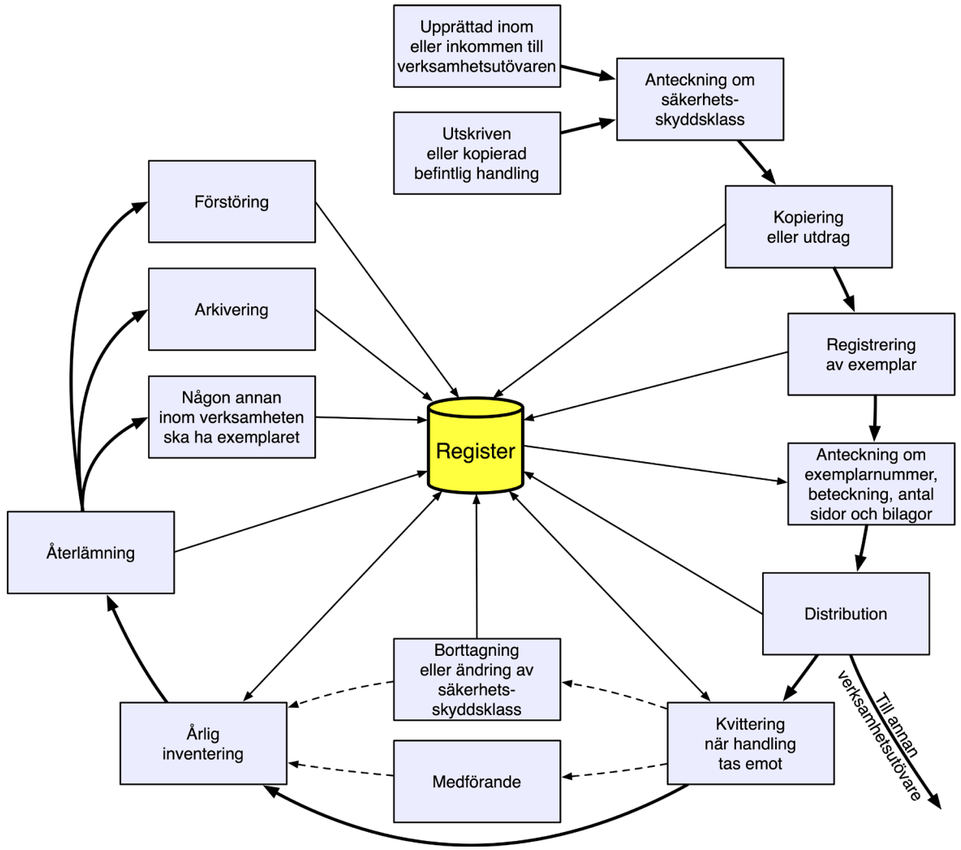
När ett exemplar inte längre behövs för arbetet lämnas det tillbaka till verksamhetens centrala funktion för hantering av säkerhetsskyddsklassificerade handlingar, som uppdaterar registret med att det har återlämnats. Ett vanligt förfarande är att originalet av den säkerhetsskyddsklassificerade handlingen bevaras, medan alla kopior förstörs efter att de har återlämnats. Dubbletter och kopior av säkerhetsskyddsklassificerade handlingar hos statliga myndigheter kan normalt gallras.

Ett exemplar förstörs så att uppgifterna inte kan återskapas. För pappershandlingar sker det normalt i en dokumentförstörare med spån som är så små att de inte kan pusslas ihop. Även förstöringen av exemplaret dokumenteras i registret. Cirkeln sluts för just det exemplaret.

Säkerhetsskyddsbehovet kvarstår efter arkivering

Ska ett exemplar arkiveras antecknas det i registret. Livscykeln för exemplaret har inte upphört, men avstannat intill att exemplaret tas upp från arkivet för att användas på nytt.

Behovet av säkerhetsskydd upphör inte när en säkerhetsskyddsklassificerad handling har arkiverats – det är fortfarande en säkerhetsskyddsklassificerad handling. Bestämmelser om informationssäkerhet, fysisk säkerhet, personalsäkerhet m.m. i säkerhetsskyddslagen, säkerhetsskyddsförordningen och Säkerhetspolisens föreskrifter om säkerhetsskydd gäller även för de arkiverade handlingarna. Det



Livscykel med åtgärder för säkerhetsskyddsklassificerade fysiska handlingar i säkerhetsskyddsklass konfidentiell och högre. Registret över handlingarna är centralt för åtgärderna och verksamhetsutövarens kontroll över handlingarna. Pilar till och från registret visar att uppgifter om handlingar hämtas från eller skrivs till registret. Figur av Kim Hakkarainen i boken Säkerhetsskydd – En introduktion.

innebär bl.a. att arkivpersonal som kan komma åt handlingarna måste vara säkerhetsprövade och att arkivlokaler har försetts med funktioner för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan.

Informationssäkerhet för registret

Som beskrivits ovan har registret över exemplar av fysiska säkerhetsskyddsklassificerade handlingar en stor betydelse för informationssäkerheten. Därför behöver även registret omfattas av åtgärder för informationssäkerhet ur främst riktighets- och tillgänglighetsperspektiven. Registret måste vara tillgängligt för att verksamheten ska kunna hantera sina handlingar. Uppgifterna i registret måste skyddas mot obehörig påverkan, så att verksamheten kan lita på att uppgifterna är korrekta. I vissa fall kan registret också vara skyddsvärt ur ett konfidentialitetsperspektiv, eftersom registret ger en antagonist kunskap om vilka personer som har åtkomst till säkerhetsskyddsklassificerade uppgifter. Kunskap som kan underlätta för andra länders underrättelsetjänster att hitta ingångar för att få tag på den information som de vill komma över.

Källor:

Säkerhetspolisen föreskrifter (PMFS 2022:1) om säkerhetsskydd.
Säkerhetsskydd – En introduktion av Kim Hakkarainen.

Týr Cyber Defense är ett specialistnätverk som erbjuder seniora konsulter inom säkerhetsskydd, it- och informationssäkerhet. Vi är främst verksamma inom försvarsindustrin och myndigheter men hjälper även företag inom segmentet kritisk infrastruktur. Vi har erfarenhet av att ta fram informationssystem för behandling av säkerhetsskyddsklassificerade uppgifter.

Vad kan Týr Cyber Defense hjälpa till med?
- Utvärdera hanteringen av säkerhetsskyddsklassificerade handlingar och ge förbättringsförslag.
- Etablera rutiner för hantering av säkerhetsskyddsklassificerade handlingar anpassade för er organisation.
- Tolka rättsliga krav om hantering av säkerhetsskyddsklassificerade handlingar.
- Kontrollera regelefterlevnaden i hantering av säkerhetsskyddsklassificerade handlingar.
- Undersöka informationssäkerheten i informationssystem med register för exemplarhantering eller system för säkerhetskänslig verksamhet.
- Genomföra utbildningar för personal som ska hantera säkerhetsskyddsklassificerade handlingar.

Se vår webbplats tyrgroup.se och kontakta oss på: info@tyrgroup.se

Läs mer

- Säkerhetspolisens vägledning om informationssäkerhet. https://sakerhetspolisen.se/verksamheten/sakerhetsskydd/vagledningar-sakerhetsskydd.html

- Boken Säkerhetsskydd – En introduktion, av Kim Hakkarainen. https://säkerhetsskyddsupplysning.se

- Myndigheten för samhällsskydd och beredskaps webbutbildning om hantering av säkerhetsskyddsklassificerade handlingar. Utbildningen har dock inte uppdaterats enligt de regler som gäller nu. https://webbutbildning.msb.se/utb/sakhand/

Säkerhetsskyddsklassificerade uppgifter är uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400). Även företag ska använda den lagen för säkerhetsskyddsklassificerade uppgifter, även om den lagen i övrigt inte gäller för företag.

Säkerhetsskyddsklassificerade uppgifter delas in i fyra säkerhetsskyddsklasser utifrån den skada som ett röjande kan medföra för Sveriges säkerhet. Säkerhetsskyddsklasserna är:
- Kvalificerat hemlig (synnerligen allvarlig skada för Sveriges säkerhet)
- Hemlig (allvarlig skada för Sveriges säkerhet)
- Konfidentiell (inte obetydlig skada för Sveriges säkerhet)
- Begränsat hemlig (endast ringa skada för Sveriges säkerhet)

Kim Hakkarainen

Roll: Konsult inom säkerhetsskydd
Arbetsplats: Týr Cyber Defense

Han har de senaste 20 åren arbetat med kvalificerade säkerhetsskydds- och informationssäkerhetsfrågor hos myndigheter och företag, bl.a. vid den militära underrättelse- och säkerhetstjänsten. En stor del av hans arbete har bestått i att förstå regler, förmedla vad regler betyder, undersöka regelefterlevnad och skriva nya regler om säkerhetsskydd. Han är författare till boken Säkerhetsskydd – En introduktion.

Lagen, informationssäkerheten och arkivarien

Vad får en arkivarie att byta sida och gå över till informationssäkerhetslaget? Är det ett omvälvande byte av värdegrund? Är det ett akut behov av nya spännande verktyg och metoder? Eller är det helt enkelt för att söka en ny väg att uppfylla gamla behov?

Under alla mina år som arkivarie har arkivhandlingarna varit centrum i mitt arbete. Oavsett om det handlat om att diarieföra, ordna, gallra eller lämna ut så har det handlat om att informationen på handlingarna ska hanteras korrekt: det ska gå att läsa, förstå, hitta och lita på äktheten i informationen. Den ska även vara tillgänglig för rätt person vid rätt tidpunkt. Det vi strävar efter är en säker hantering av informationen i arkiven – informationssäkerhet. Hur många gånger behöver man uppfinna hjulet?

Samtidigt har det under åren skett stora förändringar i hur informationen skapas och sprids. Definitionen av en allmän handling består men hur den kommer till har förändrats. Det var förr en mer avgränsad början och slut- handlingarna skrevs direkt på papper och när utformningen var godkänd betraktades den som upprättad och därmed en allmän handling. Idag uppstår handlingarna snarare i en utdragen process, skrivarbetet görs digitalt och det är inte alltid helt uppenbart när en handling är att betrakta som upprättad. Det kan skapas många olika kopior och alltför ofta sparas även olika versioner som med tiden också kan bli betraktade som slutversioner. En liten del av all den här informationen som skapas utgörs av allmänna handlingar men största delen är bara ”lös information” som inte har en uttalad status om man ser det från ett arkivhanteringsperspektiv. Man kan säga att synen på informationens liv i organisationen gått från att ha ett linjärt perspektiv till ett livscykelperspektiv.

Digitaliseringen av informationshanteringen och att hanteringen flyttat ut i molnbaserade miljöer har medfört nya typer av hot och risker. Man har en minskad kontroll över vilka vägar informationen tar och vem som har åtkomst till eller rätt att utöva kontroll över informationstillgångarna. I stället för att verkligen analysera den nya situationens risker och möjligheter så har arkivmyndigheterna till stor del nöjt sig med att deklarera att alla gamla föreskrifter och anvisningar ska betraktas som ”teknikneutrala”. Vi ska alltså ta det gamla regelverket och läsa det på ett nytt sätt, i en viss utsträckning fungerar det men i det långa loppet är det inte hållbart.

Att säkerheten är en mycket större fråga än bara allmänna handlingar och samlingarna i arkiven blev jag snabbt varse när jag fick ett uppdrag inom den civila beredskapen, för att upprätthålla robusthet inom elektronisk kommunikation . Det var oerhört lärorikt för mig som arkivarie att se svagheter inom infrastrukturen, och gav mig insikt i hur lätt slarv, godtrogenhet eller nonchalans mot den egna organisationens regelverk kan ställa till problem – även på nationell nivå.

Vid det här laget hade också ledningssystemen och standarder för informationssäkerhet börjat ta plats i myndigheternas medvetande. Och om jag får tillåta mig en cynisk iakttagelse … det som sålde in hos ledningarna var nog begreppet ledningssystem, för att ett system löser alla problem, det är känt sen länge. I det här fallet var systemet dock inte ett it-system utan ett system av roller, funktioner, styrdokument och rutiner som i grunden bygger på sunt förnuft, arkivförnuft vill jag påstå. Många av rutinerna var redan inarbetade på myndigheterna av registratorer och arkivarier. Avseende styrdokument tog Riksarkivet, Statskontoret och MSB ett framsynt grepp för att få en bättre och enad informationsstyrning på myndigheterna genom införandet av den nya processbaserade informationsredovisningen. Det har tagit många år men nu har de flesta statliga myndigheter en ny struktur för sin informationsredovisning och även många regioner och kommuner har antagit modellen. Detta av den enkla anledningen att man ser att det är en bra modell som uppfyller många av behoven för styrningen av den digitala informationshanteringen. Organisationer som följt Riksarkivets modell och som tagit fram en klassificerings-

” En svaghet hos arkivregelverket, trots de starka lagarna och föreskrifterna kring hur handlingar ska hållas skyddade, tillgängliga och läsbara är att man oftast begränsar det till arkivmaterialet, det är endast de allmänna handlingarna som omfattas.”

struktur baserad på verksamhetens processer, en dokumenthanteringsplan med anvisningar om hur varje enskild handlingstyp i varje specifik process ska hanteras och en förteckning över den information man har är på god väg att uppfylla även standardens krav på informationsstyrningen.

Vad är det då som skiljer? Varför räcker det inte med att följa antingen arkivreglementets krav eller ISO-standardens krav? Som jag ser det finns det tre saker som skiljer dem åt. Och att de skiljer sig beror antagligen mer på förhållningssätt hos människorna i systemet och deras val av tolkning än i regelverken i sig.

En svaghet hos arkivregelverket, trots de starka lagarna och föreskrifterna kring hur handlingar ska hållas skyddade, tillgängliga och läsbara är att man oftast begränsar det till arkivmaterialet, det är endast de allmänna handlingarna som omfattas. Men fram till dess att utkast och arbetsmaterial har fått statusen upprättade handlingar så hanteras de ganska respektlöst i organisationen. Ofta ligger de på någon form av fillagringsyta, i molnet eller kanske helt lokalt på handläggarens egen dator. Ju fler platser man har möjlighet att lagra på desto större risk är det att man inte hittar ens dokumentet man jobbat med 8 minuter tidigare, för det har lagt sig någon annanstans är man trodde… Det är inte säker hantering av information! I dokumenthanteringsplanerna ges sällan anvisningar om var utkast och arbetsmaterial ska lagras och hur de får spridas. För dokumenthanteringsplanerna omfattar endast arkivhandlingar, alltså de upprättade eller inkomna allmänna handlingarna. På informationssäkerhetssidan däremot jobbar man med all information, oavsett status,

eftersom även ett utkast kan innehålla känsliga uppgifter som måste tas om hand. En viktig regel här är också att inte spara utkast och handlingar med kortsiktigt värde längre än de behövs, man ska inte låta dem ligga kvar på servrar eller system som en belastning för säkerheten.

Standarden ställer stränga krav på förvaltning och uppföljning av styrdokument och rutiner. Organisationen måste tillsätta en förvaltningsorganisation med definierade roller som håller dokumentationen uppdaterad och som även övervakar efterlevnaden. Motsvarande tanke finns i arkivverksamheten, arkivredovisningens dokument är ”levande” och ska förvaltas och versionshanteras för att alltid vara aktuella. Men det finns inga krav på vilka roller som ska ingå i förvaltningen och hur det rent praktiskt ska gå till. I praktiken är det ofta arkivarien ensam som går runt i verksamheten och frågar om det skett några förändringar i processerna eller om nya handlingstyper upptäckts.

Den tredje stora skillnaden upplever jag ligger i vilket syfte man har för att upprätthålla en säker informationshantering. För arkivorganisationen är målet att bevara de allmänna handlingarna för alltid, i säkert förvar så att informationsinnehållet inte kan förvanskas eller förstöras. Syftet med bevarandet är att informationen ska vara tillgänglig för allmänheten, verksamheten och framtida forskare, såväl nu som i framtiden.

Informationssäkerhetsperspektivet har mer ett här-och-nu-intresse, informationen ska vara läslig och tillgänglig för personer som har rätt behörighet under den tid den har ett aktivt värde i verksamheten. Informationssäkerhet skyddar alltså främst informationen för dess egen skull, för att den har ett värde för verksamheten och produktionen. Men när den inte längre har ett värde för verksamheten kan den antingen göras svår att komma åt (t.ex. i ett arkiv) eller raderas beroende på hur den fortsatta behovsbilden ser ut. Informationssäkerhet är resurskrävande på flera olika sätt och därför ska man inte belasta organisationen med information som inte längre används.

Jämför det med arkivverksamheten som bevarar så mycket information som möjligt för all framtid för att någon längre fram kanske vill forska på just det ämnet. Arkivverksamheten bevarar för framtidens eventuella intresse medan informationssäkerhetsverksamheten främst ser till organisationens aktiva behov av informationen.

Hur är det då med informationens livscykel? Om man har ett cykliskt perspektiv på livet så har det ingen klar början eller slut, det rullar bara vidare. För att uppnå en livscykelhantering av informationen behöver vi alltså förena de två världarna, informationssäkerhetsperspektivet som omfattar all information, oavsett i vilken form eller vilket skede den befinner sig i och arkivverksamheten som bevarar även för framtida intressenters och forskares mer svårförutsedda behov.

Gemensamt för båda ”informationsåskådningarna” är den stora svagheten att systemet är beroende av de människorna som fyller rollerna i förvaltningen, styrningen och det löpande linjearbetet. Det är lätt att påvisa ett behov av ökad säkerhet och starta upp ett projekt som levererar de önskade styrdokumenten och rutinerna. Men att verkligen upprätthålla efterlevnaden av dem är en helt annan sak, det löpande arbetet i verksamheten kräver sin tid och icke-akuta sällanuppgifter får ofta vänta. Den organisation som certifierat sig för ISO 27000 måste visa dokumentation över att man utfört åtgärderna men det är fortfarande få myndigheter som tagit de kostsamma certifieringarna utan de väljer i stället att ”följa standarden” och då har man inga uppföljningskrav. Arkivverksamheten ska på samma sätt följas upp genom regelbundna inspektioner från arkivmyndigheten, men även här saknas resurser och det finns myndigheter som inte har inspekterats på decennier. En svaghet med inspektionerna är dessutom att trots att lagen ställer krav på arkivmyndigheterna att utföra inspektionerna ges inga andra möjligheter till sanktioner eller viten än att beslagta arkivet, vilket snarare kan ses som en möjlighet än en risk hos den inspekterade myndigheten som underlåtit att uppfylla kraven som ställs på dem.

Vad säger då arkivarien som gick över gränsen och hittade informationssäkerhetslaget? Är gräset grönare på andra sidan? Måste det vara två skilda världar, motsatt syn på informationens syfte, och krävs verkligen två olika kompetenser?

Jodå, gräset är väldigt grönt på bägge sidor, arbetet kommer aldrig att ta slut för vare sig arkivarier eller informationssäkerhetsexperter, men oavsett var gräset växer så kräver det kontinuerlig skötsel för att inte mossa och maskrosor ska ta över. Det får absolut inte heller vara två skilda världar! För att uppnå en kvalitetssäker livscykelhantering för all information behövs både arkivets långtidsperspektiv och säkerhetsexpertens snabba insatser för att hålla informationen tillgänglig och skyddad i stunden. Oavsett hur det ser ut rent organisatoriskt är ett kontinuerligt samarbete kring allt som påverkar styrning, hantering och lagring av information en förutsättning för att uppnå en säker och hållbar informationsförvaltning.

Däremot anser jag att kompetensen behöver ha olika inriktningar för att säkerställa hela livscykeln. Arkivariens kompetens inom informationsvärdering för att särskilja gallringsbar information från information som ska bevaras för all framtid är ovärderlig. Väl genomförd informationsvärdering kommer att vara en förutsättning för att det digitala arkivmaterialet ska gå att vårda och återanvända i framtiden. Vi kan inte fortsätta de senaste decenniernas maniska bevarande av data bara för att det finns gott om lagringsutrymme, och i ärlighetens namn, slippa stå till svars för gallringsbeslut som någon forskare kanske ifrågasätter medan vi ännu lever. Där vill jag ge informationssäkerhetsexperterna rätt i att vi inte ska spara onödig information, för allt vi sparar måste förvaltas och lagras på ett säkert sätt. Digital långtidslagring ställer också särskilda krav på struktur, metadata och lagringsformat. Specialistkompetens inom detta återfinns i arkivverksamheten.

Specialisten på informationssäkerhet har å sin sida kunskap om de nya hot och risker som finns och ständigt förnyas. Informationssäkerhet innebär mer än bara ISO-standard, det är en del av en övergripande säkerhetsfråga som blir allt mer komplex genom digitalisering, globalisering och inte minst den osäkra situationen i omvärlden som omfattar allt från fysisk krigföring till belastningsattacker mot det civila samhällets resurser. Så visst behövs olika kompetenser, syften och synvinklar på informationshanteringen för att vi inte bara ska uppnå utan även upprätthålla en säker livscykelhantering av informationen. Vi behöver en samlad informationsförvaltning för att säkerställa att vi samarbetar och alltid är på bettet för att hitta nya lösningar för en säker och hållbar arkiv- och informationshantering.

Martina Engsjö-Lindgren

Arkivarie. Jobbat som arkivarie, registrator, e-arkivarie, verksamhetsutvecklare, tillsynschef – det finns så många roliga inriktningar man kan välja som arkivarie! Jobbar idag på ArkivIT som senior arkivkonsult, håller dock på att smyga över till det oerhört spännande området informationssäkerhet.

Mitt råd till alla arkivarier ute på fältet är att ta för sig, vi arkivarier har en stor kompetens och är ofta de som känner till organisationen allra bäst. Sätt inte ”ljuset under skäppan”, kliv in i diskussionerna och visa var både skåpet och servern ska stå, men var alltid öppen för diskussion.

Informationssäkerhet som tjänst

Vår erfarenhet är att många organisationer vill stärka sin informationssäkerhet. Men ofta vet man inte riktigt hur man ska börja eller att ingen har tid att driva frågan.Vanligt är också att arbetet påbörjats men avstannat.

Informationssäkerhet (Infosäk) som tjänst vänder sig till organisationer som behöver externt stöd för sitt arbete med informationssäkerhet. Information är en av organisationens viktigaste tillgångar. All information måste skyddas på olika sätt och det finns även lagkrav för detta.

De flesta organisationer har någon form av regler, formella eller informella, hur man vill skydda sin information. I takt med digitalisering och teknikutveckling ökar kravet väsentligt kring skyddet. Vi på ArkivIT är experter inom informationshantering, med en bred kompetens inom olika områden och branscher.
Vi jobbar med såväl offentliga som privata organisationer.

Läs här *https://arkivit.se/tjanster/informationssakerhet/ för mer information*

ArkivIT

ArkivIT fortsätter växa och söker fler kompetenta kollegor!

Utvecklas inom arkiv och informationshantering hos ArkivIT. Tillsammans med andra duktiga specialister hjälper vi varandra i arbetet för att uppnå goda resultat. Hos oss får du vara med och bidra till innovation inom arkiv- och informationshantering på ett bolag med hög medarbetarnöjdhet.

Nu söker vi fler konsulter som arkivarier, registratorer, dokumentcontrollers, systemutvecklare, projektledare och informationssäkerhetsspecialister.

Gå in på **jobb/arkivit.se** för mer information och kontaktuppgifter.

ArkivIT är ett snabbt växande företag som är ledande på att tillhandahålla kvalificerade konsulttjänster inom digital arkiv- och informationshantering.

Välkommen på releasefest!

ArkivIT bjuder in till releasefest för att fira nya numret av **Arkiv Information Teknik** 1/23 med tema **informationssäkerhet**

Var/När:

STOCKHOLM, 20/9 2023, kl 17.30
ArkivIT, Brunnsgatan 13

GÖTEBORG, 4/10 2023, kl 17.30
Hotel Pigalle, Södra Hamngatan 2A

MALMÖ, 5/10 2023, kl 17.30
Hotel MJ's, Mäster Johansgatan 13

Kvällens talare:

Martina Engsjö Lindgren, ArkivIT
som kommer att prata om hur det är att gå från arkivarie till infomationssäkerhetsspecialist och vad som skiljer de två yrkena åt.

Andrew Tutt-Wixner, Leksands kommun
som kommer att prata om olika synsätt gällande molntjänster från ett informationssäkerhetsperspektiv. Under kvällen kommer han även att dema sitt nya verktyg för digitalisering av betyg.
https://archivetools.itch.io/digiarchive

Se fram emot:
Vi bjuder på lättare mingelmat, snacks och dryck (alkoholfria alternativ finns).

Anmälan:
O.S.A. på länken eller QR-koden senast 13 september för Stockholm och 27 september för Göteborg och Malmö *https://arkivit.se/nyheter*

Övrigt
Eventet är helt kostnadsfritt och du får jättegärna bjuda med en kollega.

Frågor?
Har du frågor om eventet får du gärna kontakta
matilda.ortenmark@arkivit.se
alexandra.meija@arkivit.se

Med vänliga hälsningar,
Vi på **ArkivIT** & redaktionen på
Arkiv Information Teknik

arkiwera

Under festen har ni möjlighet att få en kort demo av Arkiwera – en ny spännande tjänst för arkivering av era webbplatser och sociala media

Anmäl dig här