Säkerhet är pengar

Informationssäkerhet är konsten att se till att information finns där den ska, när den ska och som den ska. Om information hamnar i fel händer kan vara förödande för vissa, när den inte finns när den behövs kan det hota liv och fel information vid fel tillfälle kan orsaka felaktiga beslut som kostar en hel del pengar.

Information är idag en handelsvara och kanske den allra viktigaste anledningen till varför det gäller att ha kontroll på sin egen information. Med detta som grund är det tydligt att systematiskt riskbaserad informationssäkerhet behöver vara en naturlig del av verksamheten.

Systematiskt arbete med riskbaserad informationssäkerhet innebär att vi tar ett helhetsgrepp för att skapa ett fungerande och hanterbart arbetssätt så att den information vi har, får det skydd den behöver.

Vad är information eller informationstillgångar? Information blir användbar när förmågan och kunskapen att tolka den finns. En karta är ingen karta för den som inte lärt sig hur man skall översätta de olika symbolerna till dess mening.

Företag och myndighet samlar på sig väldigt mycket information. Information i pappersform, digital form, kunskap och erfarenhet hos nuvarande och tidigare medarbetare, men även i form av utrustning, arbetsredskap och utsmyckning. Denna information behöver struktureras för att bli användbar samtidigt som dess skyddsvärde behöver definieras

Informationssäkerhet – en naturlig del av verksamheten

I dagens och morgondagens samhälle behöver verksamheter hantera all typ av information på ett effektivt sätt, dels negativ men inte minst positiv information. Men positiv information är inte lika lätt att få ut som t ex nyheter. Vem bryr sig om ett bolag vars kunder aldrig fått sina kontokortsnummer exponerade? Eller det flygbolag som aldrig störtat? ”Quantas never crashed”. Förmågan att få ut information om positiva egenskaper kring kostnader som alla anser givna, är en konst. Kan vi tjäna pengar på arbetet med informationssäkerhet? Standardisering, så som ISO 27001, förenklar arbetet kring informations-

POSTADRESS
Box 38
745 21 Enköping

BESÖKSADRESS
Basaltgatan 3

TELEFON
0171-17 05 00

E-POST
info@basalt.se

WEBB
www.basalt.se

BASALT

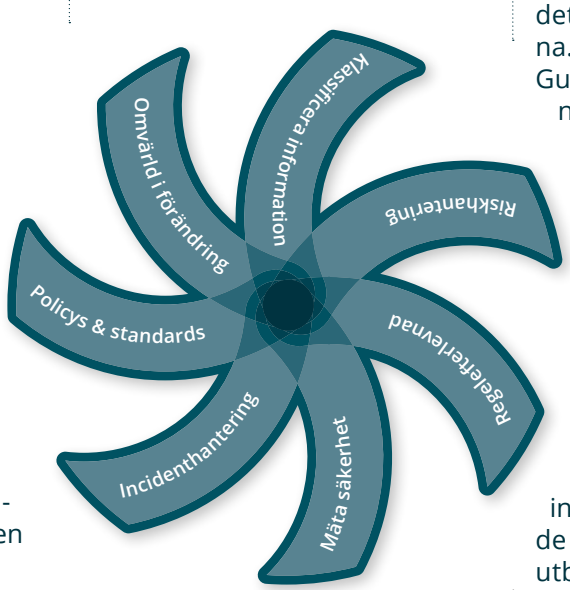
säkerhet då flera andra aktörer gör motsvarande jobb, lagar/regulatoriska krav tvingar oss till anpassningar men starkast är drivkraften att säkra verksamheten och stärka det egna varumärket.

Informationssäkerhet kan liknas med vindflöjel med sju blad, försvinner ett blir det skevt. Drivkraften att hålla hjulet i rullning är kunderna, lagar och viljan/önskan att den egna verksamheten skall uppfattas som en trygg och säker partner/leverantör/myndighet.

I princip allt arbete som systematiseras, utförs i cykler. Man börjar med att planera arbetet, utför åtgärder utifrån planeringen, kontrollerar att uppnått effekt nåtts, och agerar baserat på resultaten. Detta är den väl kända PDCA-cykeln.

Genom systematisering av riskbaserat säkerhetsarbete nås både kontroll av och kunskap om den verkliga temperaturen på organisationens verkliga säkerhetsmedvetande. Att få säkerhet att bli en naturlig del av det dagliga arbetet är lika viktigt som att digitalisering blir det. Det ger vinster i form av t ex tydlighet och trygghet.

Ett systematiskt säkerhetsarbete innebär att man arbetar med klassificering av information, riskhantering, mätinstrument, riktlinjer och regelverk, incidenthantering, medvetande och utbildning samt efterlevnadskontroll men även med hanteringsregler. Dessa åtgärder skapar tillsammans en kontrollerad säkerhetsvärld och hjälper både företag och medarbetare att göra rätt. Det måste, för alla, vara lätt att göra rätt.



OMVÄRLD I FÖRÄNDRING

Världen runt omkring oss är i ständig förändring. Vissa saker kan vi påverka, andra inte. En tydlig trend i det svenska samhället är digitalisering. Men vad är det egentligen, digitalisering? Från början handlade digitalisering om att gå från den analoga världen till den digitala, t ex klockor. Betydelsen av ordet digitalisering förändras även den, och idag, 2018, handlar det om att införa informationsteknik (IT) i verksamheten, en omvandling av verksamheten med andra ord. Detta kommer föra in oss ytterligare in i informationssamhället.

Sverige har sedan 2015 en digitaliseringsminister, och under 2018 startade Digitaliseringsmyndigheten sin verksamhet. Målet med denna myndighet är gemensam utveckling av förvaltningsgemensamma lösningar för det offentliga Sverige.

I och med digitalisering, finns även möjlighet att öka tillgängligheten på information, både inom det privata och det offentliga verksamheterna. I samband med stormen Gudrun 2005, kunde de flesta notera sårbarheter inom den digitala världen, så ock vid terrorattacken i Stockholm 2017. Under båda dessa händelser slogs mobilnäten ut. Det lev näst intill omöjligt vid dessa, och andra tillfällen, att nå och få information.

I samband med terrorattacken i Stockholm spreds det även en hel del felaktig information om vad som hände och var det skedde. Panik utbröt på flera platser i city, men även en bra bit utanför citykärnan fick den inkorrekta informationen stor påverkan på allmänhetens agerande.

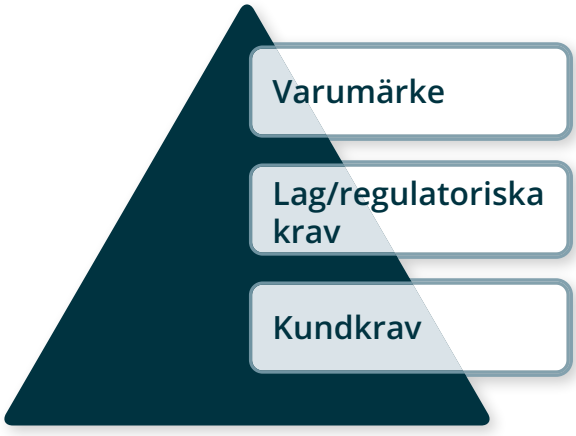
Detta visar vikten av att information som finns är korrekt. Vem ska man tro på?

Som tidigare beskrivits är information idag en handelsvara. Mycket av dagens samhälle baseras på information och hur vi agerar på information belyser vikten av att den är korrekt. En ny trend är spridningen, eller kanske mest omskrivandet kring, desinformation, ”fake news”. Det är ingenting nytt med desinformation men det har nu hamnat högt upp på många ledares agendor.

KLASSIFICERING AV INFORMATIONSTILLGÅNGAR

Vikten av att skydda den information man äger blir tydlig både för nationer och företag, men även för den enskilda individen.

För att vara säker på att informationen skyddas på ett adekvat sätt, behöver vi först och främst veta vilken information



som finns, hur pass känslig den är och vem som äger informationen. I detta arbete är det viktigt att inte skjuta över målet, det är bara information som får oacceptabla konsekvenser på verksamheten som ska skyddas. Resten av informationen ska ses som öppen eller begränsad.

Att klassificera information har varit (och är) vanligt inom försvaret. Där används hemlig /TOP SECRET, hemlig/SECRET, hemlig/CONFIDENTIAL och hemlig/RESTRICTED. Inom den privata sektorn används ofta Publik, Öppen, Intern, Hemlig och Konfidentiell.

Innan en klassificering kan göras måste man dokumentera konsekvenserna om information hanteras på ett icke önskvärt sätt. En vanlig uppdelning på detta är försumbar, måttligt negativ, betydande/stor eller mycket stor. Vad som sedan skall bedömas emot kan vara t ex varumärke, externa intressenter, monetära termer, juridiska aspekter.

Kombinationen av konsekvensbedömning och klassificering av information utgör i mångt och mycket grunden till informationsklassificering.

RISKHANTERING

För att identifiera risker behövs kunskap om vad som gör ont, vad en risk är?

I standarderna som finns på marknaden används Risk = osäkerheternas effekt på mål. För många företag och myndigheter handlar det om att identifiera de händelser som antingen påverkar det årliga resultatet, varumärket eller samhället i stort.

När riskerna är identifierade behöver man analysera hur de påverkar och varför de är en risk, så att rätt motåtgärder/skyddsåtgärder kan sättas in eller byggas upp.

Eftersom världen förändras, förändras även riskerna. Dessa behöver därför kontinuerligt analyseras och hanteras. Genom ett systematiskt arbete med risker, får vi lättare att hantera oidentifierade händelser när de dyker upp. Risker vi inte tänkt på. Även under riskhantering används den gemensamma konsekvensbedömningen.

Att ha en väl fungerande process för hantering av risker, så som beskrivs i ISO 31000, kan leda till att besvärliga situationer kan hanteras snabbare, billigare och effektivare och därmed avvärjas kanske till och med innan de inträffar.

COMPLIANCE / REGELEFTERLEVNAD

Genom att systematisk och regelbundet verifiera att verksamheten följer de regler som påverkar densamma får man kunskap om det egentliga säkerhetsarbetet och vad som måste förändras eller förbättras. Det skall vara enkelt för externa revisorer att göra djupdykningar in i verksamheten för att verifiera att efterlevnaden är korrekt. Ett certifikat på väggen må vara snyggt, men som företag eller myndighet måste man också våga bjuda till för granskning och visa att det inte finns någon smutsig byk bakom certifikatet.

För att kunna mäta efterlevnaden behövs en dokumenterad process. Efterlevnad av interna och externa regelverk med hjälp av t ex nulägesanalyser och interna revisioner behöver finnas med i denna process, samt gärna information om hur avvikelser skall och bör hanteras.

MÄTA SÄKERHET

Vad är säkerhet och hur mäter man det? I det svenska språket har vi ett ord för säkerhet, medan i engelskan finns det två, nämligen safety och security. Security handlar om de skyddsåtgärder man tar till för att förhindra olyckor eller oförutsedda händelser, medan safety är den upplevda känsla som åtgärderna förhoppningsvis medför.

En upplevd känsla är svår att mäta varför de flesta mätetal kring säkerhet handlar mer om skyddsåtgärder och incidenter än den upplevda säkerheten. Dock är det viktigt att mäta säkerhet och att presentera det arbete som utförs för att säkra verksamheten så att säkerhetsarbetet blir en del av den information ledningen får del av. Säkerhet, i alla dess former, skall vara en naturlig del i den dagliga verksamheten.

INCIDENTHANTERING

Flera av de nya lagar och förordningar som beslutats om den senaste tiden, innehåller krav på incidenthantering rörande säkerhetsincidenter. En säkerhetsincident är en incident som kan ha påverkan på säkerheten i verksamheten. Antalet säkerhetsincidenter visar organisationens förmåga att förstå vad säkerhet och en incident är, inte om säkerheten är bra eller dålig.

Genom att etablera en incidentprocess för hantering av säkerhetsrelaterade incidenter ökar regelefterlevnaden. Det skapar möjligheten att följa upp incidenterna och mäta förbättringar.

POLICYS & STANDARDS

ISO 27000-standarden är basen i mycket informationssäkerhetsarbete. Ett av kraven är att det skall finnas ett ledningssystem som hanterar informationssäkerhet. Ledningssystemet kan byggas upp på ett sådant sätt att det är enkelt att lägga till och ta bort regelverk och standards för att anpassa verksamheten efter förändringar. Ett ledningssystem kan ses som en eller flera ledstänger som visar den tänkta riktningen. Det skall ses som ett hjälpmedel för att förenkla för medarbetaren att göra rätt. Vilka regler, policys och standards man väljer att implementera är upp till den egna ledningen. Hur man sedan verifierar att dessa efterlevs, är en compliance-fråga.

SÄKERHETSMEDVETENHET / SECURITY AWARENESS

”En kedja är inte starkare än sin svagaste länk” är ett citat som ofta används kring säkerhet. Ett av de enklaste och billigaste sätten att stärka kedjan är att se till att säkerhet är en naturlig del av det dagliga arbetet och att det är enkelt att lära sig mer i ämnet. Morötter är en mycket bättre motivation för att öka medvetandegraden kring säkerhet än vad hot är. Utbildning är enkelt, men kan vara tidskrävande. Det är viktigt att finna de kanaler som fungerar inom den egna verksamheten. Vilken eller vilka kanaler man väljer, spelar egentligen ingen roll, huvudsaken är att information sprids, och tas emot. Att kombinera flera kanaler torde vara det mest gynnsamma.

HANTERING AV INFORMATION

Hanteringsregler kring information bör finnas för fysiska resurser, digitaliserad information samt för hur personalen skall agera. Beskrivning av hur information av olika klassificeringar skall hanteras. Detta inkluderar t ex lagring, kommunikation, åtkomstkontroll, kryptering etc., dvs skyddsåtgärder för både information, medarbetare och lokaler så att det blir lätt att göra rätt. Alla regler skall baseras på konfidentialitet/riktighet, integritet/sekretess och tillgänglighet.

Sammanfattning /slutkläm

”Koll på läget” är något alla vill ha. Det betyder att man vet var man är stark, var man är svag och hur man kan bli bättre. Okunskap skapar okontrollerade eller oförutsedda händelser. Genom att öva, testa och utvärdera skaffar man sig kunskap. Medvetna risker är något vi alla tar, men hur långt är vi beredda att sträcka oss i dessa risker?

I ett samhälle under ständig förändring, nya möjligheter, nya hot och risker, kan vi inte sitta still och vänta på att någon annan skall ordna saker och ting för oss. Vi måste själva ta ansvar. Ta ansvar för att veta att vi gjort det vi anser vi har råd med, både i form av risker och pengar, men även valt bort sådan som vi beslutat är irrelevant eller ointressant. Vi måste ha tagit ställning.

Ställning till vad som är skyddsvärt, vad som är viktigt, hur mycket kan vi leva utan eller hur mycket får problemen kosta, hur mycket har vi råd att betala nu, och hur mycket är vi beredda att ta risken om någonting händer.

Informationssäkerhet handlar om att förstå vad vi gör, varför vi gör det och varför vi inte gör andra saker. Det handlar om koll på läget.

FÖR FRÅGOR GÄLLANDE DENNA PROCESS KONTAKTA GÄRNA:

Camilla Odenteg

Seniorkonsult *– Camilla är seniorkonsult inom informationssäkerhet. Camilla har en lång erfarenhet av att översätta verksamheters krav till fungerade säkerhetslösningar, både tekniska och administrativa, samt förmågan att omvända problem till möjligheter.*

Mobil: +46 (0)76-305 68 09

E-post: camilla.odenteg@basalt.se

Linked In: https://www.linkedin.com/in/camilla-odenteg-284658/

BASALT *är ett företag som arbetar med systemintegration. Vi bygger specialanpassade system till kunder med speciella behov. I vår produktionsfabrik tar vi helhetsansvar för produktionen, från kravanalys till drift av det färdiga systemet. Produktion fungerar som en enhet byggd av sex delar; kravanalys, systemdesign, utveckling, test, leverans och förvaltning. Vi har också en konsultenhet som bland annat arbetar med informationssäkerhet och verksamhetsskydd och med att stödja våra system. Utöver det utbildar vi användare och driftspersonal på de system vi levererar. Basalt har funnits sedan 2009. Vår systemproduktion finns i Enköping och våra konsulter har kontor i Stockholm och Karlstad.*

VÅR MISSION *är att säkra Sverige genom att erbjuda våra kunder inom samhällsviktig verksamhet nyckelfärdiga och anpassade säkra system och tillhörande tjänster.*