Hot och sårbarhetskatalog för medlemmar i Sambi

Innehållsförteckning

1. Syfte

Detta dokument listar ett axplock potentiella hot, ett antal sårbarheter samt ett urval legala krav som kan vara aktuella för en medlem i Sambi (Samverkan för behörighet och identitet inom hälsa, vård och omsorg) i dess roll som E-legitimationsutfärdare, Identitetsintygsutgivare, Attribututgivare och/eller Tjänsteleverantör. Dokumentet kan även med fördel användas av Leverantör till Medlem. Dessa listor gör inget anspråk på att vara fullständiga eller att allt som listas är relevant för varje medlem. Listan är mer tänkt att fungera som en hjälp, inspiration och checklista för riskanalysen. Medlem bör ha omvärldsbevakning för att hålla sin riskanalys aktuell då vi lever i en ständigt föränderlig värld.

2. Ansvar

Informationssäkerhet är en tvärsektoriell fråga som berör alla och det ställer ökade krav på samverkan mellan interna och externa aktörer hos medlemmen. Kunskapsuppbyggnad, uppföljning och utvärdering är centrala inslag i styrningen av denna typ av frågor vilket ställer ökade krav på ledningens förmåga att prioritera mellan och samordna olika perspektiv.

Det finns ett omfattande regelverk som behandlar informationssäkerhetsområdet. Reglerna anger bland annat vilka krav som ställs på aktörerna inom vård, hälsa och omsorg. Reglerna för medlemmen återfinns i tillitsramverket, i lagstiftning och genom förordningar m.m. Vissa myndigheter har också utfärdat föreskrifter och allmänna råd.

Vad gäller att ta fram risk-, hot- och sårbarhetsanalyser, samt vidta säkerhetsåtgärder för att komma till rätta med brister är arbetet baserat på verksamhetsansvaret och ansvarsprincipen. Verksamhetsansvaret innebär att varje enskild medlem är ansvarig för att den egna informationssäkerheten är tillräcklig utifrån den dagliga verksamhet medlemmen bedriver. Ansvarsprincipen innebär att den medlem som normalt ansvarar för en verksamhet har samma ansvar att informationssäkerheten fungerar även under en krissituation. Därför genom verksamhetsansvaret och ansvarsprincipen har medlemmen ett åtagande att aktivt samverka med andra medlemmar och federationsoperatören för att kunna lösa sina uppgifter.

3. Risk

Medlemmens dimensionering av ledningssystemet för informationssäkerhet ska ske mot informationssäkerhetsrisken via en riskanalys. Inom IT-säkerhet betraktas risken som något dåligt. Risken kan utryckas i form av kombination av hot och sårbarhet (risk = hot x sårbarhet) där risken blir sannolikheten för att ett givet hot realiseras och därmed uppkommande skada. Denna skada kan vara mot hälsa eller liv, men också annat som exempelvis skada på personlig integritet, ekonomi, förtroende eller miljö.

Fastställande av risken sker med hjälp av en riskanalys, den som söker förslag till en enkel metod rekommenderas att ta till sig MSB dokumentet Riskanalys[1]

3.1. Skyddsvärde

Skyddsvärde används för att filtrera risker. Medlemmen behöver vid riskanalysen ta hänsyn till skyddsvärdet eftersom av legala eller andra orsaker, exempelvis vid behov av tillgänglighet, är värt mer att skydda än annat.

4. Skada

Skadan är konsekvensen av att en risk realiseras. Vård, hälsa och omsorg regleras av en mängd olika krav, interna som externa (inklusive legala). Att förlora förmågan att uppfylla ställda krav, oavsett om dessa är utryckta i text eller som våra implicita förväntningar, kan resultera i skada hos användarorganisation eller tjänsteleverantörer men även tredjepart kan ta skada exempelvis patienten vars personliga integritet blir kränkt.

[1] MSB dokument för ”Riskanalys” återfinns som en del av metodstödet på webbplatsen https://www.informationssakerhet.se/

4.1. Legala krav

Arbetet inom vård, hälsa och omsorgssektorn regleras i viktiga delar av krav i lagstiftningen. Lagar och föreskrifter kan innehålla krav som behöver tas med i riskanalysen och som därmed kan påverka organisationens ledningssystem för informationssäkerhet (LIS). Medlemmen uppmanas därför att försäkra sig om att ha en lista av lagar och föreskrifter som är relevanta, kompletta och aktuella för den egna verksamheten. Som hjälp, inspiration och checklista vid riskanalysen har det sammanställts ett extrakt av lagar som är aktuella inom vård, hälsa och omsorgssektorn. Några av de viktigaste lagarna inom sektorn är (listan uppdaterades senast 2015-02-19):

- Personuppgiftslag (1998:204)
- Patientlag (2014:821)
- Apoteksdatalag (2009:367)
- Lag (2005:258) om läkemedelsförteckning
- Lag (1996:1156) om receptregister
- Patientsäkerhetslagen (2010:659)
- Förordning (2006:196) om register över hälso- och sjukvårdspersonal
- Socialtjänstlagen (2001:453)
- Lag (2001:454) om behandling av personuppgifter inom socialtjänsten
- Förordning (2001:637) om behandling av personuppgifter inom socialtjänsten
- Lagen (1993:387) om stöd och service till vissa funktionshindrade
- Patientdatalagen (2008:355)
- Offentlighets- och sekretesslag (2009:400)
- Smittskyddslagen (2004:168)
- Lagen (2008:286) om kvalitets- och säkerhetsnormer vid hantering av mänskliga vävnader och celler
- Lagen (1993:584) om medicintekniska produkter

5. Hot

Att medlemmen ska eftersträva god informationssäkerhet handlar inte bara om att följa de regler som finns för verksamhetens skull. I dagens samhälle är tillgång till tillförlitlig information, ofta i realtid, en kritisk resurs. Hot är en möjlig, oönskad händelse med negativa konsekvenser för verksamheten.

En stor del av den information som skapas och lagras i systemen är viktig och samtidigt känslig. Åtkomst till system inom vård, hälsa och omsorg bygger på att identiteter och behörigheter kan fungera. Personuppgifter innehåller integritetskänslig information, vilket därför omgärdas av särskild lagstiftning inom vård, hälsa och omsorg. Det handlar exempelvis om informationen i beställningssystem, patientjournaler, utredningar eller forskningsverksamhet. Andra exempel på känslig information rör exempelvis medicintekniska tjänster, personalregister och förhållanden som rör läkemedel. Är informationen förlorad, stulen, manipulerad eller spridd till obehöriga kan det få allvarliga följder. Dessutom tillkommer att beroenden och kopplingar mellan olika tekniska system mellan medlemmarna är en sårbarhetsfaktor i sig genom att störningar kan få konsekvenser som både är svåra att förutse och hantera som också ökar risken för att verksamheten inte kan bedrivas på ett tillfredsställande sätt om inte IT-verksamheten fungerar.

5.1. Hotaktörer

Det grundläggande problemet avseende informationssäkerhet är att det för en hotaktör räcker med ett hål för att ta sig in medan medlemmen måste hantera samtliga möjliga svagheter. Dessutom kan medlemmen endast testa och skydda sig mot de svagheter som han känner till.

Resurserna som finns tillgängligt hos hotaktören för att genomföra hotet har stor variation avseende omfattning, kapacitet, konsekvens, tillfälle och uthållighet. Detta medför att sannolikheten och konsekvenserna för varje hot måste analyseras även där intentionen för hotaktören kan vara svår att prediktera, exempelvis för hårdvarufel i en databasdisk som hör till en molntjänst. En kvalificerad aktör kan lägga resurser på att kartlägga en unik eller okänd säkerhetsbrist samt utveckla egna innovativa verktyg för att exploatera denna. Detta kan utmynna i ett instrument som skulle kunna vara verksamt för intrång, och därpå följande extraktion av information ur i princip samtliga nätverk som tillämpar hård eller mjukvara som bär på säkerhetsbristen. Vad som gör till verklighet ett hot varierar från stater och statsunderstödda aktörer, terrorister, organiserad brottslighet till fel och störningar som inte orsakas av antagonister utan beror på mjuk- eller hårdvarufel, processbrister, bristande kvalitetskontroll, slarv, missbedömningar eller rena olycksfall. Dessutom finns det hot och risker som inte uppstår på grund av angrepp, utan snarare på grund av organisationens egna misstag och bristfälliga riskhantering.[2]

Exempel på hotaktörer:

- Nuvarande och tidigare anställda
- Patienter, nuvarande och tidigare
- Hackers, enskilda och organisationer
- Kriminella, enskilda och organisationer
- Hårdvara
- Mjukvara

[2] Informationssäkerhet – trender 2015
Myndigheten för samhällsskydd och beredskap (MSB)
Publ.nr: MSB779 - januari 2015
ISBN: 978-91-7383-509-1

- Infrastruktur
- Myndigheter, forskare samt andra organisationer, interna som externa
- Pressen och andra nyfikna
- Konkurrenter
- Naturen och miljön

Men även där verksamheten styrs av tydliga regler så kan det uppstå en värdekonflikt i utförandet. Instruktionerna som förväntas gynna hög informationssäkerhet kan hamna konflikt med användarens önskemål, exempelvis att lätt minnas sitt lösenord. Där den som utlöser en händelsekedja inte ens är medveten om sin aktörsroll, exempelvis genom att utnyttja återanvända lösenord vilket sänker eller helt undanröjer kontrollen som ska ske vid inloggning.

Därför räcker det inte bara med att analysera ett yttre eller inre hot utan även hur regler och metoder som förväntas vara riskreducerande fungerar i praktiken i stort hos medlemmen och hos den enskilda medarbetaren samt hos leverantören. Detta medför också att uppföljning och förbättringar av ledningssystemets tillämpning har stor betydelse för att minska på riskerna.

5.2. Hotlista

För att genomföra en riskanalys behövs en aktuell lista på relevanta hot. Nedanstående lista av hot speglar främst strukturen i standarden ISO27002, ”Informationsteknik-Säkerhetstekniker-Riktlinjer för informationssäkerhetsåtgärder”. För att förenkla listan så har inte varje hot tagits upp överallt även om hotet är applicerbar på flera eller alla rubrikerna. Detta medför att behovet av att bedöma hotets omfattning, kapacitet, konsekvens, tillfälle och uttålighet är något som bör utföras som en naturlig del av riskanalysen. Listan bör kunna fungera som en hjälp, inspiration och checklista vid insamling av underlag till riskanalysen. Här följer en lista av hot:

5.2.1. Informationssäkerhetspolicy

Avbrott eller fel hos affärsprocesser
Avsaknad av eller felaktig riskanalys
Ej utförd eller felaktig informationssäkerhetsanalys

5.2.2. Organisation av informationssäkerhetsarbetet

Avsaknad av informationsägare
Avsaknad av kunskap om processer, processteg och rutiner
Avsaknad av processteg och rutiner för att göra tillräcklig hantering i samband med projektavslut, avslutad anställning eller avslutat uppdrag
Avsaknad av processteg och rutiner för att göra tillräckligt kravarbete i samband med projektering, inköp eller utveckling
Avsaknad av rutin för hur datorskärmar, tangentbord och informationsbärare placeras i utrymmen med yttre insyn
Avsaknad av systemägare
Avsaknad av, ofullständiga eller felaktiga styrdokument
Delade ansvarsförhållanden
Ej utdelat ansvar

Felaktig kunskapsnivå
Felaktiga behörighetstilldelningar
Företagsbrottslighet
Gruppkonton som saknar ansvarig ägare
Informationsägare som inte känner till sitt ansvar
Kompetensutarmning
Nyckelpersonberoenden
Oklara ansvarsförhållanden
Otillräcklig kompetensförsörjning
Permanent eller temporär frånvaro eller underskott av personal
Processer, processteg och rutiner är ej dokumenterade, har ofullständig eller felaktig dokumentation
Resursbrist
Styrdokument som saknar förankring
Systemägare som inte känner till sitt ansvar

5.2.3. Personalsäkerhet

Ansvar för anställdas aktiviteter
Bedrägeri
Cyberstalking
Diskriminering
Fysiskt överfall för att komma åt eller skada information
Försäkringsbedrägeri
Hämnd mot arbetsplats
Manipulering
Mänskliga fel
Pandemier och sjukdom
Passiv-aggressivt beteende
Rättssak mot arbetsgivare
Skandaler
Tjänstefel
Vandalism
Vårdslöshet

5.2.4. Hantering av tillgångar

Angrepp med hjälp av eller via sociala applikationer
Angrepp med hjälp av eller via sociala metoder
Användarfel
Att kompromettera konfidentiell information
Avsaknad av eller felaktig informationsklassning
Avsaknad av eller felaktig rutin för informationsklassning
Avsaknad av eller felaktig systemklassning
Avsaknad av eller felaktiga rutiner för destruktion av information och informationsbärare
Avsaknad av eller felaktiga rutiner för gallring av information

Avsaknad av eller felaktiga rutiner för systemklassning
Bakdörr / fallucka
Bedrägeri
Brott mot lagstiftningen
Dirty tricks
DNS attack
Dålig publicitet
Exponera affärshemligheter
Exponera strategi och nya produkter
Förskingring
Förfalskning av register
Försäljning av stulen informationen
Illegal infiltrering
Immaterialrätt stöld
Industrispionage
Informationsläckage
Information utpressning
Insider röjer skyddsvärd information till obehörig
IP spoofing
Hemsida förvanskning
Man-in-the-middle-attack
Mutor
Missbruk av informationssystem
Nätverks sniffning
Oavsiktlig förändring av data i ett informationssystem
Oavsiktligt röjande av skyddsvärd information
Obehörig användning av upphovsrättsskyddat material
Obehörig åtkomst till informationssystemet
Obehöriga ändringar av poster
Obehörig fysisk tillgänglighet till information
Patentintrång
Phishing
Prisövervakning
Spam
Spionprogram
System manipulering
System penetrering
Skador orsakade av tredje part
Smutskastning
Social ingenjörskonst
Spioneri

Stöld
Söker upp konfidentiella information för egen eller andras vinning
TCP / IP-kapning
Tillgrepp av forskningsresultat
Tjuvlyssning
Trojan
Upphovsrättsintrång
Utläggning och hantering av skyddsvärd information på projektplatser
Utlämnande av information
Utpressning
VPN tunnel kapning Virus
Worms
Återspelningsattacker

5.2.5. Styrning av åtkomst

Avsaknad av eller felaktig rutin för besökshantering
Avsaknad av eller felaktig rutin för policy/rutin Rent skrivbord och tom skärm
Avsaknad av eller felaktig rutin för skärmlåsning eller lösenordslåst skärmsläckare
Avsaknad av eller felaktiga rutiner för att ta bort icke aktiva användare
Dold eller falsk användaridentitet
Felaktig behörighetsadministration
För höga behörigheter hos användare
För höga behörigheter hos personal i helpdesk
För höga behörigheter hos personal som arbetar med testning
För höga behörigheter hos personal som jobbar med utveckling
Hanteringen av gruppkonton saknar eller har felaktiga rutiner
Lösenordsattack
Utlämnande av lösenord utan kontroll av mottagare

5.2.6. Kryptering

Avlyssning
Avsaknad av eller felaktiga rutiner för hantering av kryptonycklar och kryptoteknik
Knäcka kryptering
Återspelning

5.2.7. Fysisk och miljörelaterad säkerhet

Avsaknad av eller felaktig rutin för brandsyn
Avsaknad av eller felaktiga rutiner för hantering av säkerhet och skydd
Blixt
Bomb attack
Bombhot
Brand
Farligt material relaterade händelser
Föroreningar, exempelvis luftburna

Skred
Soleruption
Stormar
Terroristattacker
Vandalism
Översvämning

5.2.8. Driftsäkerhet

Attacker på fysisk infrastruktur
Avsaknad av eller felaktiga rutiner för att underhålla skydd mot skadlig kod
Avsaknad av eller felaktiga rutiner för hantering av larm och akuta händelser
Destruktion av journaler
Felaktiga rutiner för kontroll av spårdata och loggar
Förlust av el
Förlust av stödtjänster
Fel på utrustning
Missbruk av releaseverktyg
Obehörig användning av programvara
Obehörig installation av programvara
Program fel
Strejk i den egna organisationen eller hos leverantör
Sabotage
Sabotageprogram
Skadlig kod
Skador till följd av penetrationstester
Strejk, arbetstagares eller lockout, arbetsgivares åtgärder

5.2.9. Kommunikationssäkerhet

Fel i kommunikationslänkar
Fysisk störning av kommunikationer
Tillgång till nätet av obehöriga

5.2.10. Anskaffning, utveckling och underhåll av system

Avsaknad av eller felaktiga rutiner för att utrangera gammal utrustning
Avsaknad av eller otillräcklig testning och kvalitetskontroll
Avsaknad av eller otillräcklig uppföljning och/eller kontroll
Avsaknad av processteg eller rutiner för att genomföra nödvändig hantering i samband med utrangering av datamedia, system eller infrastrukturutrustning
Avsaknad av rutiner för dokumentation av systemkonfiguration
Fel i underhåll

5.2.11. Leverantörsrelationer

Avsaknad av eller felaktiga avtalsvillkor på leverantör i samband med utkontraktering
Avsaknad av eller ofullständigt styrande kontrakt och avtal

Avsaknad av kravställning på leverantör i samband med utkontraktering
Avsaknad av säkerhetsbilagor till kontrakt och avtal
Avsaknad av uppföljning av existerande styrande kontrakt och avtal
Brott mot avtalsförhållanden
Ej utförd eller felaktigt utförd säkerhetsskyddad upphandling
Felaktig kravställning på leverantör i samband med utkontraktering

5.2.12. Hantering av informationssäkerhetsincidenter

Avsaknad av eller felaktiga rutiner för hantering av säkerhetsrelaterade IT-incidenter
Avsaknad av eller felaktiga rutiner för hantering av säkerhetsrelaterade IT-incidenter
Avsaknad av eller felaktiga rutiner för uppföljning av säkerhetsrelaterade IT-incidenter
Falsifierade IT-incident rapporter

5.2.13. Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet

Avsaknad av eller felaktig krishantering
Avsaknad av kontinuitetsplanering
Ej efterlevnad av kontinuitetsplaner
Ej övad kontinuitetsplanering
Felaktig eller ej uppdaterad kontinuitetsplanering

5.2.14. Efterlevnad

Avsaknad av rutiner för kontroll av spårdata och loggar
Ingen uppföljning eller utvärdering av effekt, kvalitet eller konsekvens hos processer, processteg eller rutiner

6. Sårbarhet

Sårbarhet inom informationssäkerhet är svaghet gällande en tillgång eller grupp av tillgångar, vilken kan utnyttjas av ett eller flera hot som därmed exponerar organisationen för en risk. Därför är sårbarhet den sammanvägda bilden av vår förmåga att skydda system, infrastruktur, verksamhet eller information utifrån säkerhetsmedvetande, tillgängliga resurser och exponeringen i tid och rum.

6.1. Sårbarhetslista

Genom att förstå sårbarheten så öppnas möjlighet att hantera risken. Nedanstående lista av sårbarheter speglar främst strukturen i standarden ISO27002, ”Informationsteknik-Säkerhetstekniker-Riktlinjer för informationssäkerhetsåtgärder”. Dessa presenterade sårbarheter gör inget anspråk på att vara en komplett lista eller att samtliga sårbarheter är relevanta för medlemmens verksamhet, resurser eller information. Listan bör fungera som en hjälp, inspiration och checklista vid insamling av underlag till riskanalysen. Här följer en lista av sårbarheter:

6.1.1. Informationssäkerhetspolicy

Affärsprocess förändring saknar eller brister i informationssäkerhetsanalys
Affärsprocess har brister

Brist på intern dokumentation
Brist på riskanalys
Bristande tillgång till styrande regler och instruktioner samt kontrollregler
Otillräcklig förändringsledning
Otillräckligt säkerhetsmedvetande
Otillräckliga affärsregler
Otillräckliga affärsstyrning
Processer som inte tar hänsyn till mänskliga faktorer

6.1.2. Organisation av informationssäkerhetsarbetet

Avsaknad av eller felaktig skräpposthantering
Anslutning av personliga enheter till företagsnätverket
Brist på informationssäkerhetsmedvetande
Brist på rutiner för att scanna in information
Brist på rent skrivbord och tydlig tom skärm policy
Diskutera information på offentliga platser E-posta dokument med information
För mycket behörighet i en person
Förlora säkerhetsdosor, mobiltelefoner (läsplatta, laptop) med säkerhetsappar eller autentiseringskort såsom ID-kort
Installera otillåten programvara eller appar
Interaktion med kunden
Lagrar information på mobila enheter som mobiltelefoner, läsplattor, laptop, etc
Låta obehöriga få tillgång till arbetsplatsen
Otillräcklig åtskillnad mellan olika funktioner
Skicka och dokument Skriva ner lösenord och känslig information
Social interaktion
Ta bort eller inaktivera säkerhetsverktyg
Tillgång till information utanför kontoret (papper, mobiltelefoner, bärbara datorer)

6.1.3. Personalsäkerhet

Brist på eller för låg påföljd när man inte följer informationssäkerhetspolicy och regler
Brister i rekryteringsprocessen
Omotiverade anställda
Otillräcklig utbildning av medarbetare
Otillräcklig övervakning av anställda
Saknar positiv motivering för att följa informationssäkerhetspolicy och regler
Tidigare anställda som arbetar för konkurrenter
Tidigare anställda behåller företagets information
Tidigare anställda diskuterar organisationens angelägenheter
Utför inte säkerhetsprövning

6.1.4. Hantering av tillgångar

Bristande hantering för avveckling av information
Bristande hantering kapacitet

Bristande kontroll över information som går in och ut
Enkelt att kopiera
Okontrollerad kopiering av information
Okontrollerad nedladdning från Internet
Otillräcklig klassificering av information

6.1.5. Styrning av åtkomst

Användarrättigheter inte regelbundet granskade
Brist på förfarandet för att ta bort åtkomsträttigheter vid uppsägning
Brist på system för identifiering och autentisering
Brist på validering av behandlad information
Fildelning överrider behörighetskontrollen
Komplicerade användargränssnitt
Lösenord tillåts utan granskning av deras forceringsstyrka eller återanvändning
Medlemskap i sociala nätverk öppnar upp för informationsinsamling
Okontrollerad användning av informationssystem
Otillräcklig kontroll av fysisk åtkomst
Otillräcklig lösenordshantering
Snabba tekniska förändringar
Specialsystem som man vet för lite om
Tekniska hinder för att åstadkomma önskad styrning
Webbläsare

6.1.6. Kryptering

Brist på policy för användning av kryptografi
Otillräckligt skydd för kryptografiska nycklar

6.1.7. Fysisk och miljörelaterad säkerhet

Kontor och datacenter anläggningar vars placering är så att de kan ta skada av naturkatastrofer
Opålitliga strömkällor
Otillräcklig fysiskt skydd
Otillräckligt kablage säkerhet
utanför Sveriges gränser
Platsen sårbar för översvämningar
Platsen är lokaliserad i område med hög brottslighet
Platser som är politiskt instabila
Platser under statlig spionerі, exempelvis där kommunikation, systemdelar eller tjänsten utförs
Samlar kritisk eller all information i samma geografiska plats
Utrustning känslighet för fukt och föroreningar
Utrustning känslighet för temperatur

6.1.8. Driftsäkerhet

Brist på backup
Brist på redundans

Bristande underhåll
Fel i systemdriften
Felaktig konfiguration av hårdvara
Hårdvara känslighet för damm, värme och fukt
Hårdvara med konstruktionsfel
Konfigurationsfel och missade säkerhetsmeddelanden
Missat säkerhetsuppdateringar
Otillräcklig eller oregelbunden backup
Otillräcklig IT-kapacitet
Utgången eller inte underhållen hårdvara
Utrustning känsligheten för förändringar i spänning

6.1.9. Kommunikationssäkerhet

Alltför stora privilegier
Använder Wifi-nät
Använder Bluetooth kopplade tangentbord
Brist på skydd för mobil utrustning
Oskyddad nätverkskommunikation
Osäkra nätverksarkitektur
Outnyttjade användar-ids
Onödiga jobb och skript som utför uppgifter på information eller konfiguration
Oskyddade offentliga nätverksanslutningar
Otillräcklig nätverkshantering
Vidareförmedlar organisationens nätverk via egen router exempelvis i mobila enheter som mobiltelefoner, läsplattor, laptop, etc
Öppna fysiska anslutningar, IP-adresser och portar

6.1.10. Anskaffning, utveckling och underhåll av system

Avyttring av lagringsmedia utan att radera information
Brist på verifieringskedja
Kunderna har tillgång till säkra områden
Kundens tillgång till information (exempelvis via kundportal)
Odokumenterad programvara
Otillräcklig ersättning av äldre utrustning
Otillräcklig förändringsledning
Otillräcklig segregering av operativa- och testanläggningar
Otillräcklig testning
Oskyddad användarinmatning
Otillräcklig testning av programvara
Programvarubuggar och konstruktionsfel
Programvara som inte tar hänsyn till mänskliga faktorer
Programvarans komplexitet

Programvara som en tjänst (överlåtit kontrollen av information)
Programleverantörer som går i konkurs eller byter ägare

6.1.11. Leverantörsrelationer

Avsaknad av eller bristfällig support på levererad programvara och tjänster
Delar konfidentiell information med partners och leverantörer
Dålig val av testdata
Försörjningsavbrott på information
Levererad programvara är buggig
Ofullständig specifikation för programvaruutveckling
Otillräcklig övervakning av leverantörer
Partners och leverantörer saknar eller brister i informationssäkerhet
Störningar av telekomtjänster
Störningar av allmännyttiga tjänster såsom el, gas, vatten

6.1.12. Hantering av informationssäkerhetsincidenter

Otillräcklig incident och problemhantering

6.1.13. Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet

Brist i kontinuitetsplanering

6.1.14. Efterlevnad

Brist på regelbundna revisioner
Brist på eller dålig tillämpning av internrevision
Övertro på säkerhetsgranskningar

7. Appendix – Riskanalysens arbetsuppgifter

Fastställande av risken sker med hjälp av en riskanalys. Detta appendix visar ett förslag till hur detta görs med den metod som rekommenderas i MSB dokumentet Riskanalys[3], kapitel 3, Riskanalysens arbetsuppgifter. Övriga avsnitt i dokumentet avseende förberedelser och sammanställning hänvisas direkt till källan.

Välj och beskriv analysobjektet

Bestäm dig för vad som ska analyseras, exempelvis attributkälla och intygsutgivare.

Flera analysobjekt

Har du flera objekt att analysera så beskriv objektet och dess avgränsningar. Ta ett objekt i taget, exempelvis: attributhantering för tillfälligt anställda.

Identifiera hot och sårbarheter

Hotlistan är lång, välj ut vilka hot är relevanta för objektet som ska analyseras. När du ser listan så känner du kanske igen några hot som redan har inträffat och några som kan inträffa. För detta analysobjekt så upplevs nedanstående hot under rubriken ”Styrning av åtkomst” som relevanta:

- Felaktig behörighetsadministration
- För höga behörigheter hos användare

Om någon av ovanstående hot inträffar, ställ frågan vilken skada som kan orsakas om hotet realiseras, exempelvis gör en tydlig beskrivning ”att med för höga behörighet så kan en medarbetare få tillgång till att ändra information som är förbjudet enligt lagstiftningen”.

Sårbarhetslistan hanteras på motsvarande sätt ger förslag på sårbarheter i analysobjektet, vad det är som kan ge en öppning i analysobjektet, exempelvis så kan följande vara relevanta:

- Användarrättigheter inte regelbundet granskade
- Brist på förfarandet för att ta bort åtkomsträttigheter vid uppsägning

Beskriv vad det finns för sårbarheter i analysobjektet som är relevant, exempelvis: användarrättigheter för tillfälligt anställda som återkommer på nytt till arbetsplatsen återfår de behörigheter som personen hade förut.

[3] MSB dokument för ”Riskanalys” återfinns som en del av metodstödet på webbplatsen http://www.informationssäkerhet.se

Att tänka på i gruppdiskussionen

Dokumentera hotet och sårbarheten, gå vidare i att söka fler hot och sårbarheter i analysobjektet, lämna lösningstänket till senare, gör bilden tydlig så att deltagarna förstår sammanhanget.

Sammanställ och gruppera hot

Ta bort dubbletter och förbättra beskrivningarna. Få till en komplett lista av hot och sårbarheter som kan grupperas ihop, vissa kan överlappa varandra, ett hot kan angripa flera sårbarheter eller olika kombinationer av hot och sårbarheter.

Bedöm risken – konsekvens och sannolikhet

Konsekvensen av att ett hot realiseras är en beskrivning av skadan. Skadan kan bli verklig på många olika sätt, exempelvis så kan en person få fel roll i systemet men som i all välvilja skriver in en upplysning som av andra uppfattas som diagnos resultera senare i en allvarlig skada hos en patient. Förslag på att gradera konsekvensen:

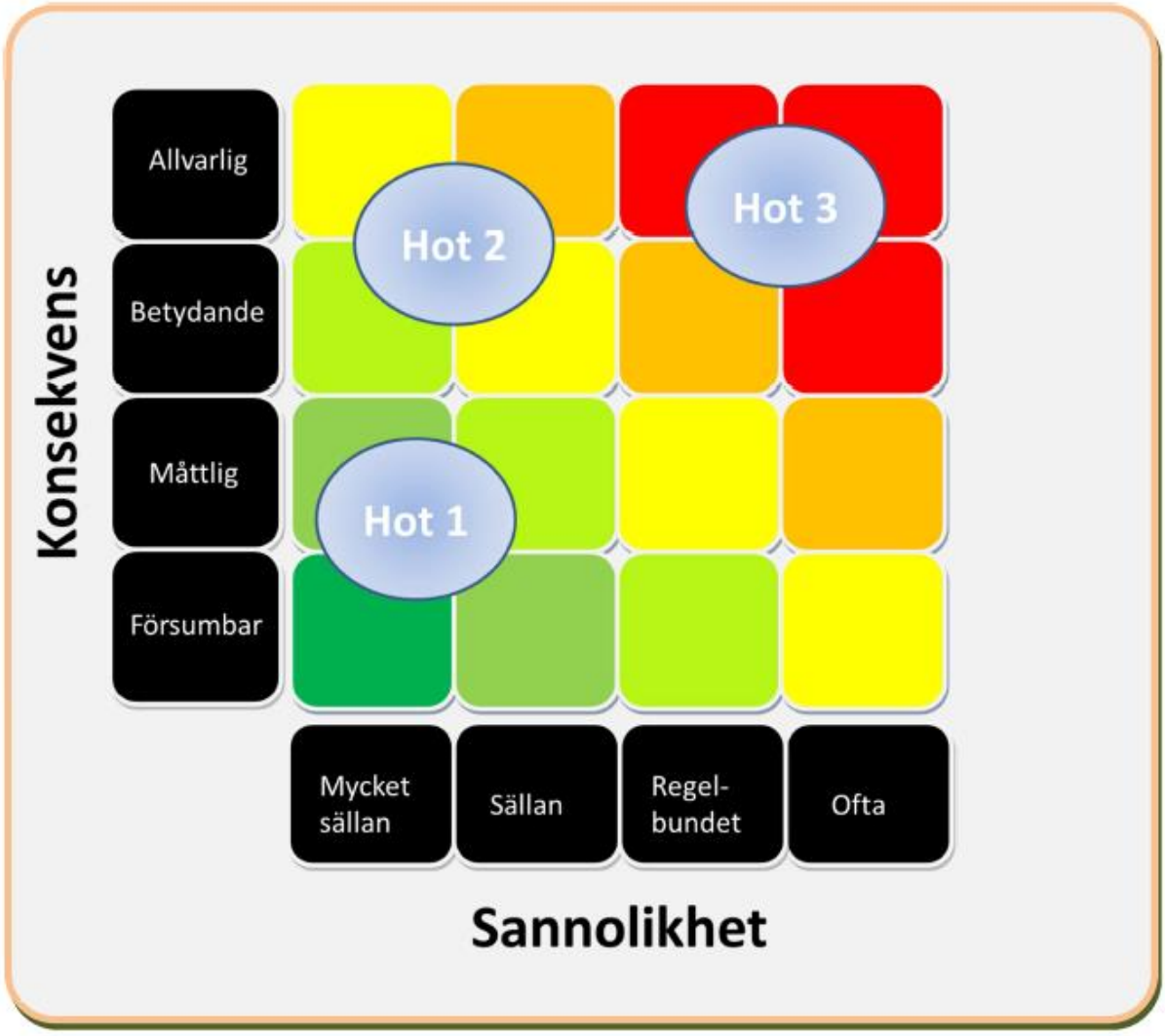
- försumbar skada
- måttlig skada
- betydande skada
- allvarlig skada

När säkerhetsåtgärden är stark så kanske hotet inträffar mycket sällan men är sårbarheten stor hos analysobjektet så ökar sannolikheten att hotet kan penetrera sårbarheten. Förslag på att gradera sannolikheten att hotet kan penetrera sårbarheten:

- mycket sällan – en gång på 100 år
- sällan – en gång på 10 år
- regelbundet - årligen
- ofta – mer än en gång per år

Inplacering av hoten i en matris

Skapa en matris och placera in identifierade hot och sårbarheter utifrån deras konsekvens (den skada de kan tillsammans åstadkomma) och sannolikhet, se figuren nedan:



Figur 1 Matris med inlagd hot och sårbarhet

Det kan behövas flera matriser för att täcka ett analysobjekt och ha olika matriser för varje analysobjekt.

Ta fram åtgärdsförslag – prioritera

Matrisen visar var det finns högst risk. Skyddsvärdet kan variera och behöver tas i beaktande när man prioriterar i vilken ordning åtgärdsförslag tas fram.