Microsofts molntjänster & svenska krav på integritet och patientdatasäkerhet

Microsoft

Om detta White Paper

Organisationer inom sjukvårdssektorn pressas ständigt till att använda sina resurser så effektivt som möjligt. En lösning är ofta att använda mer IT och teknik för att effektivisera sin verksamhet. Samtidigt måste organisationer inom sjukvårdssektorn följa alla svenska bestämmelser kring integritet och säkerhet för hälsoinformation.

För många beslutsfattare inom sjukvården väcker tanken på molntjänster kanske frågor om säkerhet, integritet och ägandeskap. Frågor som ofta grundar sig i missuppfattningar om hur molntjänster fungerar.

Microsofts molntjänster är säkra, juridiskt trygga och lika flexibla och skalbara som el- och vattenförbrukning. Detta till skillnad från att ha sin egen hårdvara, vilket kräver resurser, binder kapital och skapar ett ständigt behov av service och underhåll.

Detta White Paper riktar sig mot beslutsfattare och IT-ansvariga på sjukhus, apotek, vårdcentraler, etc och deras leverantörer. Den ger en kort översikt av bestämmelserna på området, en detaljerad analys av hur Microsofts molntjänster är utformade för att följa dessa bestämmelser, samt information om hur specifika erbjudanden kan användas av svenska sjukvårdsorganisationer och deras leverantörer för att hitta lösningar som följer alla bestämmelser.

Sammanfattningsvis gör Microsofts molnlösningar det möjligt för sjukvårdsorganisationer att fokusera på sin kärnverksamhet, utöka sina tjänster och minska sina kostnader – samtidigt som dessa organisationer kan luta sig mot oöverträffad säkerhet, kontroll och juridisk trygghet.

Innehållsförteckning

Om detta White Paper 2
MICROSOFTS MOLNTJÄNSTER 4
INLEDNING 4
INTRODUKTION AV SVENSKA SJUKVÅRDSREGLER 6
DET VERKLIGA HOTET MOT SÄKERHETEN OCH INTEGRITETEN FÖR ELEKTRONISK PATIENTHÄLSOINFORMATION 8
SÅ BYGGER VI IN OCH UPPRÄTTHÅLLER SÄKERHETEN I MICROSOFTS MOLNINFRASTRUKTUR 9
Microsofts Online Services Trust Center 10
Microsofts Azure Trust Center 10
SÅ INTEGRERAS OCH UPPFYLLS SÄKERHETEN I MICROSOFTS PLATTFORMAR OCH TJÄNSTER 11
Microsofts® Security Development Lifecycle (SDL) 12
Best practice för säker utveckling av Windows Azure-applikationer 13
Automatisk kontroll av säkerhetskrav 13
Active Directory 13
Automatiseringsverktyg för säkerhet 14
SVENSKA REGLER FÖR PATIENTSÄKERHET OCH INTEGRITET 15
Smartguide för säkring av affärsinformation 15
Kryptering 15
Resurser 16
Hur använder jag smarta krypteringstekniker för molnapplikationer? 16
FIPS-validerade kryptografibibliotek 16
Skydd av data under överföring 17
Identifiering och autentisering 18
Resurser 18
Windows Identity Foundation förenklar användartillgång för utvecklare 18
Inloggning och bevakning 18
Resurser 19
Ta kontroll över loggning och spårning med Windows Azure 19
Motståndskraft 20
Affärskontinuitet 20
Geografisk lättillgänglighet 20
Finansiellt garanterat servicenivåavtal för onlinetjänster 20
FÖRTJÄNAR DIN TILLIT – FÖRSTÅR PROBLEMOMRÅDET 21
SLUTSATS 22
Vi är Microsoft in Health. 22
Om detta dokument 23

MICROSOFTS MOLNTJÄNSTER

Microsofts strävan är att vara en nära samarbetspartner till företag och organisationer. Vi använder spetsteknologi inom mjukvara kombinerad med många års erfarenhet för att hjälpa till att implementera de tekniska, fysiska och administrativa säkerhetsåtgärderna som krävs för sjukvårdsrelaterad information i Sverige.

Microsoft skapar säkerhet och integritet i systemet genom att kombinera säkerhetsfunktioner i vår programvara med de säkerhetsåtgärder som finns i våra datacenters och administrativa processer. Våra kunder får möjlighet att kontinuerligt följa regelverket samtidigt som de kan dra full nytta av valet att använda lösningar som bygger på våra molntjänstplattformar.

INLEDNING

I dag ställs sjukvårdsorganisationer inför stora utmaningar när det gäller att minska kostnader och komplexitet samtidigt som innovation och samarbete ska främjas. De måste leverera sjukvård av hög kvalitet, hålla nere kostnader och samtidigt arbeta förebyggande med patienterna för att främja folkhälsan. Apotek måste leverera medicin till sina patienter på ett så säkert och effektivt sätt som möjligt. Programvaruleverantörer som riktar sig mot sjukvården vill ofta erbjuda produkter som ökar komplexiteten istället för att stegvis bygga på det som redan finns. Myndigheter behöver analysera patientinformation för att förbättra sjukvården. Sist men inte minst finns det många nystartade sjukvårdsaktörer som vill utöka sina tjänster för att nå en större marknad, men som avskräcks av den kostnad och de resurser som krävs för att skapa och sköta den IT-infrastruktur som deras tillväxtambitioner fordrar.

De här utmaningarna görs ännu större av kraven på att följa regelverket kring säkerhet och integritet vid hantering av skyddad hälsoinformation. Det svenska regelverket om integritet och hälsoinformation finns bl.a. i patientdatalagen och apoteksdatalagen. Ansvaret för att säkerhets- och integritetsbestämmelserna följs läggs på en rad olika sjukvårdsaktörer, liksom på de underleverantörer som kommer i kontakt med elektronisk patienthälsoinformation.

Arbetsplatsens IT-infrastruktur kan göra det svårare att följa lagarna, på grund av säkerhetsbrister, försummelser och stöldrisker. Svaret på de utmaningar som utgörs av kostnader, komplexitet och behovet av innovation och samarbete ligger i att använda sig av kraften i molnet. Molnet kan leverera informations- och kommunikationsteknik som täcker allt från samarbete, kunskapshantering, kommunikations- och automatiseringsverktyg till katastrofsäkring och högprestandanät för forskning. Och det som en skalbar, automatiserad, fullt tillgänglig, kostnadseffektiv, underhållsfri och behovsdimensionerad tjänst.

Neelie Kroes, vice ordförande i EU-kommissionen, skriver på sin blogg: (http://ec.europa.eu/commission_2010-2014/kroes/en/blog/e-health-for-savings)

"I en fallstudie från 2008 visades att den årliga kostnaden per patient kunde sänkas med 36,7 % med hjälp av e-hälsolösningar. Om e-hälsolösningar skulle implementeras över hela Europa så är det mycket möjligt att européernas sjukvårdskostnader skulle minska istället för att öka de närmaste åren. I tider av finansiell åtstramning och stigande budgetunderskott är det ofta mer effektivt att spendera smartare istället för att spendera mindre. EU:s digitala dagordning, som jag ansvarar för, har satt som tydlig strategi att IT-möjligheter ska utnyttjas till fördel för det europeiska samhället. E-hälsa är en av de mest lovande möjligheterna. Europeiska regeringar bör se framtiden an och fånga de möjligheter som informationstekniken erbjuder och förbereda sina medborgare, gamla som unga, på åren som kommer."

Sjukvårdsorganisationer är ofta tveksamma till att anförtro patientinformation till utomstående på grund av risken för stöld och förlust samt skadeståndsskyldighet. Beslutsfattare slits mellan sin önskan att dra nytta av de ekonomiska och operativa fördelarna som finns i molnet, och sin rädsla för att riskera säkerheten och integriteten för sin information.

Lösningen är att arbeta med en molnleverantör som utmärker sig i rollen som "ansvarsfull dataförvaltare" och som bygger in säkerhet och integritet i sina molnlösningar med alla administrativa, tekniska, fysiska och organisationsmässiga säkerhetsåtgärder som krävs av svenska bestämmelser för integritet och hälsoinformation.

Syftet med detta White Paper är att visa hur Microsoft byggt in säkerhet i sin molninfrastruktur genom sitt nätverk av globala datacenter (Global Foundation Services), sina plattformar för beräkningar, lagring och databaser under samlingsnamnet Azure, samt molnapplikationer som Office 365 och Dynamics CRM Online.

De här resurserna kan användas av vårdgivares IT-avdelningar eller leverantörer för att bygga lösningar som följer lagar och bestämmelser och låter vårdgivaren fokusera på sin kärnverksamhet. Microsoft har byggt in säkerhet i sin teknologi på alla nivåer och använder ett processdrivet ramverk för att se till att lösningarna anpassas löpande efter regler och bestämmelser.

Genom att arbeta med Microsoft kan beslutsfattare snabbt leverera molnbaserade lösningar med Microsofts plattformar som grund. Dessa säkerställer sekretessen, integriteten och tillgängligheten för den elektroniska patentinformationen, samtidigt som den är skyddad mot säkerhetshot.

Som exempel kan nämnas att Microsofts HealthVault är plattformen som valdes för projektet HälsaFörMig (personligt hälsokonto) under Apotekets upphandling 2013.

Detta White Paper består av fyra delar:

- Översikt av svenska bestämmelser kring integritet och hälsoinformation
- Översikt av hur Microsoft bygger in och upprätthåller säkerheten i sin molninfrastruktur, sina molnplattformar och molnapplikationer
- Så skyddar Microsoft din information
- Hur hanteras kontinuerlig efterlevnad av regelverket; Effektivt processdrivet ramverk

INTRODUKTION AV SVENSKA SJUKVÅRDSREGLER

Målgruppen för detta White Paper är beslutsfattare i näringslivet, compliance managers, programvaruutvecklingschefer, IT-konsulter och systemintegratörer som arbetar inom, eller på uppdrag av, organisationer som måste följa svenska bestämmelser kring patienters integritet och hälsoinformation. **Den här publikationen är inte avsedd att ge råd åt organisationer angående deras juridiska skyldigheter och ansvar. Det förutsätts att läsaren förstår de lagar och regler som nämns i texten och hur de lagarna och reglerna påverkar deras organisation.** För läsare som inte känner till svenska bestämmelser om integritet och hälsoinformation tillhandahåller vi en kort översikt av dessa. Läsare som redan känner till de här bestämmelserna och hur de är tillämpliga på molnlösningar kan gå direkt till nästa avsnitt.

De svenska bestämmelserna om patientintegritet och hälsoinformation finns i följande lagar och föreskrifter (en fullständig genomgång av den historiska bakgrunden och de specifika kraven i de här lagarna och föreskrifterna ligger utanför ramen för den här publikationen):

- **Patientdatalagen** gäller när en molntjänst används av en vårdgivare för att behandla hälsoinformation, i vid bemärkelse. Den begränsar de syften i vilka informationen kan behandlas och innehåller ett antal generella krav liknande de som finns i apoteksdatalagen (nedan), t.ex. skyldigheter vad gäller säkerhet, integritet och radering av hälsoinformation.
- **Apoteksdatalagen** gäller när ett svenskt apotek använder en molntjänst för att behandla hälsoinformation som är kopplad till användare av läkemedel och farmaceutiska tjänster och/eller personer som har behörighet att skriva ut läkemedel. Den reglerar behandlingen av uppgifterna i apotekens kunddatabaser och produktregister och begränsar de syften i vilka hälsoinformation får behandlas. Där slås också fast skyldigheter vad gäller

säkerhet, integritet och radering av information, liknande dem som finns i patientdatalagen (ovan).

- **Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14)** gäller för vårdgivare och fastslår vissa detaljerade krav, t.ex. att vårdgivare ska använda stark autentisering, ha en informationssäkerhetspolicy samt dokumentera och rapportera hur de uppfyller säkerhetspolicyn.

- **Patientsäkerhetslagen** kräver att privata enheter som hanterar databaser/register med hälsoinformation håller denna konfidentiell.

- **Offentlighets- och sekretesslagen** slår fast att behandling av hälsoinformation i offentlig sektor faller under tystnadsplikt och sekretess (samma regler gäller för privata vårdgivare, men det faller under patientsäkerhetslagen).

- **Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för systematiskt kvalitetsarbete** innehåller allmänna råd om ledningssystem för systematiskt kvalitetsarbete samt föreskrifter såsom att vårdgivare bara får behandla hälsoinformation när så är nödvändigt för vårdens kvalitet. Enligt dessa riktlinjer (liksom i andra relevanta lagar som anges ovan), är vårdorganisationer förbjudna att använda tjänsteleverantörer som har för avsikt att samla hälsoinformation för sina egna kommersiella syften, till exempel marknadsföring.

- **Personuppgiftslagen** innehåller allmänna krav för behandling av personuppgifter i Sverige. Den härrör från EU: s dataskyddsdirektiv (95/46/EG) och omfattar grundläggande krav för behandling av personuppgifter och särskilda underkategorier, t.ex. hälsoinformation.

Att följa lagarna, föreskrifterna och riktlinjerna ovan är av största vikt för alla vårdorganisationer i Sverige. För att kunna dra nytta av fördelarna med molntjänster måste alla vårdorganisationer först noggrant utvärdera varje molntjänst som de överväger att använda så att de kan vara säkra på att inte bryta mot några regler. Framför allt gäller det för vårdorganisationen att se till att molntjänstleverantören förstår det regelverk som bör tillämpas. Till sist bör molntjänstleverantörerna kunna verifiera att de har genomfört de åtgärder som krävs för att vårdorganisationen ska följa svenska lagar och regler.

Så uppfyller Microsoft svenska sjukvårdsreglers krav

Microsofts datacenter och tjänster är certifierade enligt säkerhets- och revisionsstandarderna ISO 27001 och SAS 70/SSAE 16. I praktiken måste varje enskild vårdgivare/registeransvarig bedöma hur Microsofts olika lösningar och

verktyg uppfyller de krav som gäller. Kunderna får göra den bedömningen från fall till fall, baserat på vilken typ av information det rör sig om, och i vilken kvantitet och med vilka metoder den behandlas och överförs.

- Microsoft har anslutit sig till Safe Harbor-principerna för databehandling och uppfyller därmed den svenska personuppgiftslagens krav på hantering av personuppgifter av företag utanför det Europeiska ekonomiska samarbetsområdet (EES).
- För att hjälpa dig att bedöma hur väl Microsofts tjänster uppfyller de svenska kraven vad gäller hälsoinformation har Microsoft utarbetat en checklista som listar de viktigaste kraven, tillsammans med Microsofts lösningar för att uppfylla dem. (se bilaga).

DET VERKLIGA HOTET MOT SÄKERHETEN OCH INTEGRITETEN FÖR ELEKTRONISK PATIENTHÄLSOINFORMATION

För många beslutsfattare i sjukvården leder tanken på "molnet" till missuppfattningar om säkerhet, integritet och ägandeskap. Baserat på intervjuer med ledningen för olika svenska vårdinrättningar har Microsoft delat upp farhågorna i olika kategorier:

1. Att hålla informationen säker

   "Jag kan inte ha patientinformation på externa servrar."

2. Förlora kontrollen

   "Även om Microsoft är ansvarig för driften så är jag fortfarande ansvarig för att säkerheten efterlevs."

3. Juridiska frågor

   "Våra jurister skulle aldrig tillåta det."

Verkligheten i dag är att elektroniska patientjournaler redan lagras utanför vårdorganisationernas väggar och att de juridiska avdelningarna godkänner detta baserat på de säkerhets- och integritetsåtgärder som lagringsleverantören demonstrerat, och på de finansiellt garanterade servicenivåavtal som de tillhandahåller. Det är viktigt att förstå vad som är det verkliga hotet mot säkerheten och integriteten för elektronisk patienthälsoinformation.

Ett av de största hoten mot säkerheten för elektronisk patientinformation är stöld, följt av obehörig åtkomst/utlämnande av informationskällor på arbetsplatsen. Stulna bärbara datorer och oskyddade pappersregister är vanliga orsaker till informationsintrång.

Den slutsats som kan dras från vårt material är att, vid tidpunkten detta skrivs, har inga intrång inträffat i en säker, publik molntjänstmiljö med rigorösa fysiska, tekniska och administrativa säkerhetsåtgärder på plats.

Vårdorganisationer som vill vidta åtgärder för att minska sin sårbarhet för kostsamma och skadliga säkerhetsintrång bör därför överväga fördelarna med att gå över till Microsofts säkra molnplattformar.

SÅ BYGGER VI IN OCH UPPRÄTTHÅLLER SÄKERHETEN I MICROSOFTS MOLNINFRASTRUKTUR

Microsofts strategi för integritet och säkerhet börjar från grunden med att säkra molninfrastrukturen. Microsoft driver ett världsomspännande nät av branschledande datacenter som skyddas fysiskt av omfattande åtgärder, såsom strikt åtkomstkontroll, biometrisk avläsning och videoövervakning. Microsoft uppfyller ISO 27001 och SAS 70/SSAE 16 standarderna för säkerhetsprocesser och revision.

Fysiska

- STRÄNG ÅTKOMSTKONTROLL
- BIOMETRISKT AVLÄSNING
- VIDEOÖVERVAKNING
- REDUNDANT STRÖM-FÖRSÖRJNING

Microsoft har också implementerat robusta säkerhetsåtgärder för data och nätverk. Bland åtgärderna kan nämnas två-faktors-autentisering, säkerhetsbevakning, risk- och sårbarhetsanalys samt system för skydd av fil- och dataintegritet.

Data och nätverk

- SÄKERHETSBEVAKNING
- RISK- OCH SÅRBARHETSANALYS
- ÅTKOMSTKONTROLL
- TVÅFAKTORSAUTENTISERING

Microsofts Facilities Access Controls och automatiserade serverhanteringssystem gör att de vanligaste orsakerna till säkerhetsintrång, fysiska stölder av hårddiskar och bärbara datorer, inte längre är ett problem för organisationer som går över till Microsofts moln. Om enstaka, fysiska kopior av elektroniska patientjournaler måste finnas så ser teknik som Microsofts BitLocker och Active Directory RMS till att dessa hanteras på ett säkert sätt.

Microsofts moln drivs av Online Services Security and Compliance (OSSC), ett team inom Microsofts Global Foundation Services Division. Teamet använder de principer och processer som Microsoft har utvecklat med hjälp av många års erfarenhet av att hantera säkerhetsrisker i traditionella utvecklings- och driftsmiljöer.
OSSC-teamet ansvarar för informationssäkerheten i Microsofts molninfrastruktur.

Genom att placera funktionen i molnet kan Microsofts molntjänster dela på samma säkerhetslösningar och minska komplexiteten och därigenom vinna stordriftsfördelar. Med det tillvägagångssättet som standard kan alla Microsofts serviceteam fokusera på de unika säkerhetsbehoven hos respektive kund.

OSSC-teamet jobbar för att ge användarna en riskfri miljö i Microsofts moln med sitt Microsoft Information Security Program som använder en riskbaserad arbetsmodell. Programmet består av regelbundna riskhanteringsgenomgångar, utveckling och underhåll av ett ramverk för säkerhetskontroll, samt pågående aktiviteter för att säkerställa efterlevnad, från att utveckla datacenter till att svara på förfrågningar från rättsvårdande myndigheter.

Teamets procedurer är *best practice* och innefattar ett antal olika interna och externa granskningar av hela livscykeln för varje onlinetjänst och för varje element i infrastrukturen. Genom att de olika Microsoft-teamen arbetar nära varandra bygger de en heltäckande strategi för att säkra applikationer i Microsoft-molnet.

När man driver en global molninfrastruktur som sträcker sig över många verksamheter finns många skyldigheter att uppfylla och som också granskas av externa revisorer. Granskningsbara krav kommer från myndigheter, branschorgan, interna policys samt från branschpraxis. OSSC-programmet garanterar att kraven efterlevs, utvärderas och införlivas fortlöpande.

Efterlevnad och certifiering

- EFTERLEVER SA270
- EFTERLEVER ISO 27001
- EFTERLEVER FISMA
- INDUSTRICERTIFIERINGAR ÄR KÄRNAN I TJÄNSTEPORTFÖLJEN
- YTTERLIGARE CERTIFIERINGAR ÄR PLANERADE

Ett resultat av Information Security Program är att Microsoft följer viktiga standarder som ISO/IEC 27001:2005 och SAS 70/SSAE 16 vilket i sin tur underlättar granskningar från oberoende, externa parter.

ISO 27001 är en certifiering för ett Information Security Management System (ISMS), d.v.s. ett system för att bevaka, mäta och styra informationssäkerheten som helhet. Det förklarar hur man använder kontrollerna inom ISO 27002 (tidigare känd som ISO 17799), vilket är en uppförandekod för hantering av informationssäkerhet.

Här finns mer information:

Microsofts Online Services Trust Center; http://office.microsoft.com/sv-se/business/office-365-sakerhetscenter-sakerhet-for-molndata-FX103030390.aspx

Microsofts Azure Trust Center; http://www.windowsazure.com/sv-se/support/trust-center/

De här certifieringarna är extra betydelsefulla i sjukvårdssammanhang eftersom det ännu inte finns några certifieringsorgan för efterlevnad av de svenska sjukvårdsreglerna. De ovan nämnda certifieringarna täcker dock en stor del av de säkerhetsåtgärder som specificeras i de svenska sjukvårdsreglerna.

SÅ INTEGRERAS OCH UPPFYLLS SÄKERHETEN I MICROSOFTS PLATTFORMAR OCH TJÄNSTER

Microsoft skiljer på Software as a Service (SaaS), Platform as a Service (PaaS) och Infrastructure as a Service (IaaS) för svensk sjukvård. För ett antal av Microsofts SaaS-erbjudanden, t.ex. Office 365, stödjer Microsoft efterlevnad på applikationsnivå och administrationsstyrning. Med dessa skyddsåtgärder på plats kan vårdsorganisationer implementera riktlinjer och rutiner som stödjer deras ansvar för fullständig efterlevnad av svenska sjukvårdsregler.

Elektronisk patientinformation som lagras på IaaS- eller PaaS-lösningar såsom Windows Azure och SQL Azure omfattas av programvaruutvecklingen hos den organisation som använder dem.

Svenska vårdorganisationer, som är ansvariga för att regelverket efterlevs i sitt moln, kan bygga lösningar på Azure-plattformen som uppfyller säkerhetskraven för svensk sjukvård. Därmed kan organisationen med rätt administrativa skyddsåtgärder och rutiner på plats använda onlinetjänster på ett sätt som är förenligt med svenska sjukvårdsregler.

Microsofts strategi för integritet och säkerhet bygger in säkerhetsåtgärder tidigt i utvecklingen av programvaruplattformarna. Det görs enligt Microsofts Security Development Life Cycle, en uppsättning procedurer och *best practice*. Dessutom förser Microsoft sina kunder med den senaste tillgängliga utbildningsinformationen via Technet-artiklar, och strävar efter att leverera ett säkert, privat och tillförlitligt datormoln via sitt **Trustworthy Computing Initiative;** http://www.microsoft.com/en-us/twc/default.aspx

I det följande avsnittet kommer detaljerna i de här tre processerna och teknikerna att gås igenom:

- Microsofts Secure Development Lifecycle, som används i utvecklingen av våra molnlösningar.
- Våra interna, automatiserade säkerhetspolicyer som används i Microsofts datacenter.
- Software Security Capabilities, en teknik som är inbyggd i våra molnlösningar och som möjliggör efterlevnad av svenska sjukvårdsregler.

Läsare som inte är intresserade av dessa detaljer kan hoppa vidare till avsnittet om affärsberedskap.

Microsofts® Security Development Lifecycle (SDL)

Figur 1: SDL-processen

När svenska vårdgivare använder en lösning i Microsofts molnerbjudande kan de vara säkra på att säkerheten byggts in i programvaruprodukten under hela utvecklingskedjan. Microsoft har utformat en säkerhetsprocess för programvaruutveckling som består av en samling säkerhetsrutiner. Grupperade efter de olika faserna i den traditionella livscykeln för programvaruutveckling. När metoderna körs i kronologisk ordning resulterar de i en mätbart högre säkerhetsstandard än vad som blir fallet vid ad hoc-utvecklad programvara.

SDL-verktygslådan och/eller de tillhörande konsulttjänsterna kan användas av programvaruutvecklare och är den metod som alla Microsofts tjänster följer för att säkerställa säker kodning och efterlevnad med Microsofts produkter. Microsofts molnplattformar har utformats med hjälp av Security Development Lifecycle (SDL). Microsoft SDL bygger på tre centrala begrepp: *utbildning,kontinuerlig processförbättring och ansvarsskyldighet*. Den kontinuerliga utbildningen av tekniska yrkesroller inom en programvaruutvecklingsgrupp är av stor vikt. Lämpliga investeringar i kunskapsöverföring hjälper Microsoft och dess partner att reagera på rätt sätt när tekniken och hotbilden förändras. Eftersom säkerhetsriskerna inte är statiska lägger SDL stor vikt vid att förstå orsak och verkan av säkerhetsproblem och kräver regelbunden utvärdering av SDL-processer och förändringar som svar på nya tekniska landvinningar eller nya hot. Data samlas in för att utvärdera utbildningens effektivitet. Mätningar under processens gång används för att kontrollera följsamheten och mätningar efter lanseringstillfället används för att ge vägledning åt framtida förändringar. Genom att kombinera med en detaljerad

beredskap- och kommunikationsplan kan organisationen tillhandahålla koncis och övertygande vägledning till alla berörda parter.

Som visas i figuren ovan delas SDL in i sju delområden, men det finns fem kärnområden som grovt motsvarar faserna i en traditionell programvaruutvecklingscykel:

- Utbildning, policy och organisatorisk kapacitet
- Krav och design
- Implementering
- Verifiering
- Lansering och respons

Här följer en beskrivning av några av de säkerhetstekniker som programvaruutvecklare bör använda, och de säkra design- och utvecklingsmetoder de ska använda för att bygga säkrare Windows Azure-applikationer.

Best practice för säker utveckling av Windows Azure-applikationer

Automatisk kontroll av säkerhetskrav

När vårdorganisationer använder lösningar från Microsofts molnprodukter får de automatiserade säkerhetsåtgärder från Microsoft via Active Directory och dess utbud av verktyg för sårbarhetsavläsning och uppdatering.

Active Directory

Microsofts produktteam använder Active Directory Domain Services (ADDS), som central plats för konfigurationsinformation, autentiseringsförfrågningar samt de objekt som är lagrade i Active Directory av pålitliga domäner. Genom att använda Active Directory kan Microsofts produktteam effektivt hantera användare, datorer, grupper, applikationer och andra katalogaktiverade föremål från en säker, centraliserad plats.

Active Directory Group Policy-inställningar används av Microsofts produktteam för att verkställa säkerhetsåtgärder; det kan röra sig om tidsbegränsade lösenord, komplexitet, längd, historik, och återanvändbarhet. Säkerhetsinställningarna för Active Directory är konfigurerade för att hämma försök att få obehörig åtkomst till resurser i domänen. Dessa konfigurationer kräver att användaren har en unik identifikation för sitt personliga bruk, användning av lämpliga tekniker för att verifiera den påstådda identiteten hos en användare och systeminloggningsrutiner som minimerar spridning av information om systemet, för att inte hjälpa individer som försöker få obehörig åtkomst. Active Directory-gruppolicyerna är också utformade för att säkerställa integriteten för medlemmarnas servrar i deras område genom att föra ut klocksynkronisering via domänkontrollanter. Andra säkerhetsmekanismer som tillhandahålls av Active Directory begränsar åtkomst och loggar aktiviteter.

I Microsofts fleranvändarlösningar kontrollerar och förhindrar Active Directorys Organizational Units (OU) obehörig och oavsiktlig överföring av information via delade systemresurser. Användarna isoleras från varandra baserat på säkerhetsgränser ("silos"), logiskt separerade av Active Directory.

Utöver Active Directory Domain Services ger Microsofts molntjänstprodukter bättre basfunktioner för användare som jobbar inom vården genom att stödja integration med Active Directory Rights Management Services. Active Directory Rights Management Services (AD RMS) hjälper sjukvårdsorganisationer och tjänsteleverantörer att säkerställa att endast de personer som behöver se elektronisk information om en patients hälsa kan göra det. AD RMS kan skydda en fil genom att identifiera de rättigheter som en användare har till filen. Rättigheter kan konfigureras för att tillåta en användare att öppna, ändra, skriva ut, vidarebefordra eller vidta andra åtgärder med rättighetsskyddad information. Med AD RMS kan vårdgivare säkerställa data som distribuerats utanför nätverket.

Automatiseringsverktyg för säkerhet

Alla Microsofts molntjänster prenumererar på Microsofts Security Response Service för att få säkerhetsuppdateringar, nyhetsbrev och råd. Microsoft Security Response Center (MSRC) är ett globalt team som arbetar för att garantera säkerheten vid användning av Microsoft-produkter. MSRC levererar säkerhetsuppdateringar och kompetent säkerhetsvägledning till Microsoft och Microsofts kunder. MSRC identifierar, övervakar, löser och svarar på säkerhetsincidenter och sårbarheter i Microsoft-program. MSRC hanterar även Microsofts företagsövergripande säkerhetsuppdateringsprocesser och fungerar som navet för samordning och kommunikation. MSRC släpper säkerhetsnyhetsbrev den andra tisdagen varje månad. Prenumeranter på Microsoft Security Bulletin Advance Notification får en förvarning tre bankdagar före den ordinarie säkerhetsuppdateringen släpps vilket hjälper Microsofts produktteam att konfigurera sitt infrastrukturbevakningsverktyg, QualysGuard. Microsofts molntjänster använder otaliga säkerhetsverktyg för att hjälpa till att identifiera och avlägsna risker.

Säkerhetsautomatiseringen använder verktyg för sårbarhetsskanning, uppdatering, antivirus, efterlevnad, rapportering och ärendehantering. Verktyg för sårbarhetsskanning som QualysGuard kontrollerar statusen för säkerhetsuppdateringar i molninfrastrukturmiljön. QualysGuard är ett program som dagligen utvärderar sårbarheten på applikations- och värdnivå. Verktyget uppdateras ofta för att möta kraven från den ständigt föränderliga hotmiljön. Ytterligare verktyg för sårbarhet används för webbapplikations- och databasskanning. Microsofts noggranna sårbarhetshantering gynnar direkt de svenska vårdkunder som utvecklar på Microsoft-molnplattformen eftersom deras system kommer att skannas regelbundet.

Microsofts produktteam använder ett brett utbud av saneringsverktyg för att hjälpa till att installera programfixar och tillämpliga säkerhetsuppdateringar. De verktyg som används är skalbara för att passa stora organisationer och moln, och kan rapportera

från varje enhet för sig. Alla säkerhetsuppdateringar och programkorrigeringar måste genomgå SDL-processen och rigorösa tester innan de kan driftsättas i molnmiljön.

Alla servrar i Microsofts moln har antivirusprogram som skydd mot skadlig programvara. Det antivirusprogram som Microsofts molntjänster använder är en helt centralt administrerad lösning som i realtid skannar inkommande filer, kollar automatiskt efter uppdaterade signaturfiler och programuppdateringar och rapporterar all upptäckt skadlig kod till Microsofts Operations Center (MOC).

Microsofts produktteam använder verktyg för att hålla reda på de många certifieringarna och intyg som varje produktteam har uppnått. Ett av dem är efterlevnad av de svenska sjukvårdsreglerna. Verktygen hjälper produktteamen att upprätthålla och verkställa säkerheten i hela molnmiljön.

SVENSKA REGLER FÖR PATIENTSÄKERHET OCH INTEGRITET

Säkerheten är ofta det sista man tänker på när man utvecklar applikationer och systemteknik. På Microsoft har vi byggt in många kontroller i vår molninfrastruktur och i våra plattformar för att se till att säkerheten aldrig glöms bort. Första steget vid inbyggnad av skyddsåtgärder är att klassificera informationen. Microsoft klassificerar information efter hur mycket den kan påverka verksamheten, så att känslig information kan vara väl skyddad, hanterad och övervakas med lämpliga kontroller. Här beskrivs Microsofts strategi som svenska vårdorganisationer kan utnyttja för att klassificera sin information.

Smartguide för säkring av affärsinformation

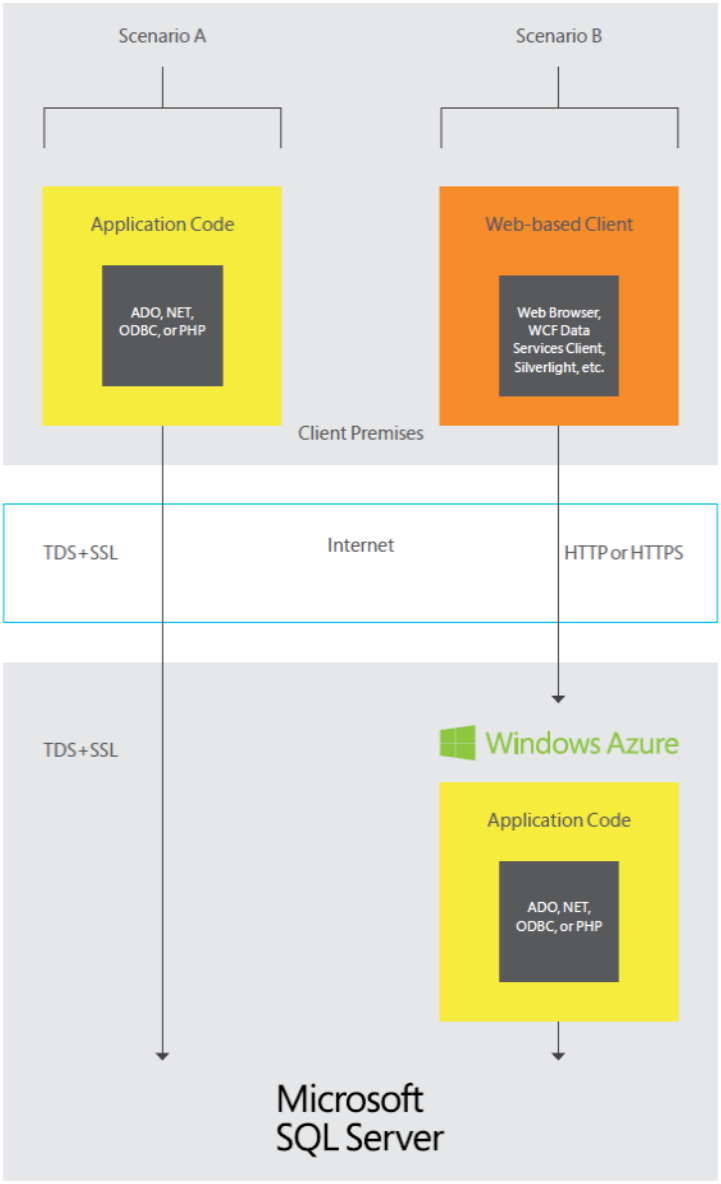
Kryptering

Microsoft erbjuder ett brett utbud av kryptografiska lösningar inom molnet och har varit ledande med att erbjuda kryptografiska bibliotek till sina kunder i flera år. I dagsläget har Microsoft 49 olika FIPS 140-2-validerade certifikat för sitt krypteringsarbete som inte bara skyddar känslig information åt Microsoft själv, utan också åt alla applikationsutvecklare som använder Microsofts plattformar, teknik och molntjänster.

Resurser

Hur använder jag smarta krypteringstekniker för molnapplikationer?

FIPS-validerade kryptografibibliotek



Windows Azure SDK utökar kärnan i .NET-biblioteket för att göra det möjligt för utvecklare att integrera och utnyttja de tjänster som tillhandahålls av Windows Azure. Det innebär att utvecklare får tillgång till alla .NET-kryptografitjänster i Windows Azure. Dessa är viktiga för att öka säkerheten i alla system för att skydda lagrad data. Genom att utnyttja SDK kan utvecklare vid svenska vårdinrättningar eller deras tjänsteleverantörer verkställa riktlinjer och rutiner som krävs för efterlevnad av de svenska sjukvårdsreglerna och se till att mekanismer införs för att kryptera känsliga data i lagring.

Ett av de verktyg som Microsoft utvecklar för att hjälpa till att säkra elektroniska patientjournaler med kryptering eller avidentifiering är Azure Trust Services.

Programmet, som av Microsoft fått kodnamnet "Trust Services", är ett ramverk för kryptering på applikationsnivå som kan användas för att skydda känsliga data som lagras på Windows Azure-plattformen. Data som krypterats med Trust Services kan endast dekrypteras av auktoriserade kunder. Det ger utgivaren av datan fria händer att distribuera den fritt efter att ha krypterat den med Trust Services. Köpare eller abonnenter av känslig data som krypterats med Trust Services kan känna sig tryggare med att informationen är intakt och att risken för att någon obehörig tillgått informationen är minimerad.

Grundscenariot består av två steg:

- Dataproducenter krypterar den känsliga datan med Trust Services och lagrar den i Windows Azure eller SQL Azure.
- Auktoriserade datakunder kan dekryptera datan efter att de läst in den från lagringen.

Endast "utgivare" och "abonnenter" till nätverksknutpunkten kan kryptera eller dekryptera data baserat på regler som fastställts av programadministratören. Trust Services-modulen själv är inte "anförtrodd" med krypteringsnycklarna. Microsoft har därmed inte tillgång till de nycklar som krävs för att dekryptera de krypterade datakolumnerna, och programutvecklaren kan se till att känsliga uppgifter såsom personnumret i en patientjournal aldrig kommer att finnas i Microsoft-system i okrypterad form och att Microsoft (våra system, anställda, leverantörer etc.) så gott som aldrig kommer att ha möjlighet att dekryptera uppgifterna.

Skydd av data under överföring

Utvecklare kan dra nytta av alla funktioner för data under överföring som finns i Microsofts molnerbjudanden. På den högsta nivån kan anslutningar över Internet använda SSL-kryptering som stöder ett brett utbud av chiffer och kan garantera integritet över internetuppkopplingen.

Dessutom stöder SQL Azure dataström i tabellform (TDS) över SSL. Det innebär att utvecklare för det mesta kan ansluta till och interagera med databasen på samma sätt som i Microsoft SQL Server. Det är definitivt värt att överväga ADO.NET-kryptering och betrodda servercertifikat, speciellt när man öppnar en SQL Azure-databas genom molnet. Anslutningsegenskaperna Kryptera = True och TrustServerCertificate = False kan i rätt kombination bidra till att dataöverföringen blir säker och förhindra ”man-in-the-middle-attacker”. Detta är också ett krav för att ansluta till SQL Azure - det är omöjligt att ansluta till SQL Azure utan krypterad anslutning.

Genom att utnyttja den här sortens krypteringsfunktioner för data under överföring kan svenska vårdorganisationer implementera riktlinjer och rutiner som krävs för

efterlevnad av svenska sjukvårdsregler och se till att mekanismer införs för att kryptera känsliga data i rörelse.

Identifiering och autentisering

Utvecklare kan använda identifiering och autentisering på applikationsnivå via Windows Identity Foundation. Det gör att .NET-utvecklare kan ge yttre form åt identitetslogik från sin applikation, förbättra utvecklarnas produktivitet, förbättra tillämpningens säkerhet och möjliggöra interoperabilitet. Dessutom erbjuder Microsoft:

- Active Directory Federation Services 2.0: en säkerhetsnyckeltjänst för teknik som ger ut nycklar och hanterar användaråtkomst och möjliggör federering och åtkomsthantering för förenklad inloggning.
- Windows Azure Access Control Services: ett enkelt sätt att ge identitet och åtkomstkontroll för webbapplikationer och tjänster, och samtidigt integrera med standardbaserade identitetsleverantörer, inklusive kataloger såsom Active Directory®, och webbidentiteter såsom Windows Live ID, Google, Yahoo! och Facebook.

Denna teknik gör att svenska sjukvårdsorganisationer och deras tjänsteleverantörer kan uppfylla det svenska regelverket för hälsoinformation.

Resurser

Windows Identity Foundation förenklar användartillgång för utvecklare

Inloggning och bevakning

Windows Azure Diagnostics gör det möjligt att samla in omfattande diagnostiska uppgifter för att stödja felsökning av en tjänst under användning. Den har stöd för en rad olika diagnostiska funktioner, inklusive Windows Azure-loggar, Windows Event-loggar, IIS-loggar, Failed Request Tracing (allmänt känt som "FREB")-loggar, minnesdumpar vid eventuell applikationskrasch och prestandaräknare, samt Windows Azure Diagnostic Monitor-loggar som ger data om funktionen. Windows Azure loggar direkt utan närmare inställningar - det är en del av Windows Azure SDK. Det finns vissa fördelar med att använda loggningsramverk som Logger.NET, Enterprise Library, log4net eller Ukadc.Diagnostics. De kan lägga till mer struktur till loggningsmeddelandena och även bidra med en del av den flexibilitet som nämndes tidigare.

I SQL Azure hanteras transaktionsloggningen automatiskt av SQL Azures infrastruktur. SQL Server Analysis and Reporting Services är tillgängligt och stöds av SQL Server 2008 R2, liknande det stöd som finns i SQL Azure. Dessutom är SQL Azure Reporting

en molnbaserad rapporteringstjänst som bygger på SQL Azure Database, SQL Server, och SQL Server Reporting Services-tekniken. Det går att publicera, visa och hantera rapporter med data från SQL Azure-källor.

Dessa skyddsåtgärder visar hur regelverket uppfylls vilket gör det möjligt för en svensk vårdorganisation att kolla systemaktivitet, loggbevaka och säkerställa revision.

Resurser

Ta kontroll över loggning och spårning med Windows Azure;

http://channel9.msdn.com/search?term=monitoring+applications+in+windows+azure&type=All

Motståndskraft

Affärskontinuitet

Affärskontinuitetsrisker, såsom hantering av säkerhetskopiering och återskapande utrustning, kan överföras genom att utnyttja Microsofts molnplattformar. Microsoft kan ge mer robusta och billigare affärskontinuitetslösningar än företag kan åstadkomma på egen hand.

När du använder Microsofts molntjänst innebär det att Microsoft tar över ansvaret för katastrofsäkringen. Microsoft tar allvarligt på katastrofsäkringsfrågan eftersom ett strömavbrott påverkar resultat.

Kontinuitet

- FLERA GEO-BASERADE DATACENTER
- ANVÄNDARE KAN VÄLJA MELLAN EN PLATS ELLER UTSPRIDDA DATACENTER
- LAGRAD DATA REPLIKERAS ÅTSKILLIGA GÅNGER
- STRUKTUREN ÄR UTFORMAD FÖR ATT SÄKERHETSKOPIERAS OCH ÅTERSTÄLLAS FRÅN KONTROLLPUNKTER

Geografisk lättillgänglighet

Applikationer kan dra nytta av datacenterspridning utan stora investeringar eller utvecklingskostnader. Microsofts molntjänster kan tillhandahålla ytterligare kapacitet på begäran. Med hjälp av molnet klarar du oförutsedda toppar i användningen då systemen återupptar arbetet efter avbrott. Det sänker också kostnaden för infrastruktur kring katastrofsäkring. Abonnenter kan ersätta delar av sin egen dedikerade infrastruktur för katastrofsäkring med Microsofts molninfrastruktur.

Finansiellt garanterat servicenivåavtal för onlinetjänster

Våra onlinetjänster är utformade för att leverera pålitlighet, tillgänglighet och prestanda med 99,9 % upptid och finansiellt garanterade servicenivåavtal (SLA).

FÖRTJÄNAR DIN TILLIT – FÖRSTÅR PROBLEMOMRÅDET

Microsoft har över 90 000 anställda som vi försäkrar, och vi har därför en unik position i vilken vi själva måste ta itu med utmaningar kring efterlevnad av regelverket såsom svenska bestämmelser kring integritet och hälsoinformation, samtidigt som vi också möter dessa frågor via våra produkter och tjänster. Svenska vårdorganisationer kan dra nytta av Microsofts erfarenhet av att uppfylla regelverket då dessa stärker våra produktteam. På Microsoft tror vi på att hålla oss till samma standard som våra kunder gör, vilket innebär att vi är mycket väl positionerade för att förstå utmaningarna som svenska vårdorganisationer möter.

SLUTSATS

Som ansvarsfull rådgivare till våra kunder och partner inom vårdsektorn förstår Microsoft vikten av att skydda elektronisk patienthälsoinformation. Vi delar dina förpliktelser gentemot patienterna och vi garanterar att de strategier och processer för efterlevnad vi har som din affärspartner är i linje med dina egna metoder och din roll som svensk vårdorganisation.

Med det sagt så vill vi stödja vårdsektorn genom att förändra synen på informationsteknikens roll. Med vårt breda utbud av flexibla datormolnserbjudanden och plattformar som går från IaaS, PaaS till SaaS och deras inbyggda säkerhetsfunktioner, gör vi det möjligt för våra partner att uppnå kostnadsbesparingar, affärsflexibilitet och skalbarhet och självklart stöd för att uppfylla svenska bestämmelser om integritet och hälsoinformation.

Microsoft hjälper dig att klara de fysiska, tekniska, administrativa och organisatoriska skyddsåtgärder som krävs av svenska vårdorganisationer med hjälp av:

- ✓ Molninfrastrukturer, -plattformar och -programvaror med inbyggda säkerhets- och integritetskontroller
- ✓ En programvaruutvecklingsprocess som bygger in säkerheten från första början
- ✓ Automatiserade säkerhetsfunktioner i driften av våra datacenter
- ✓ Kontinuerligt uppdaterad säkerhetsteknik i framkant, integrerad i våra produkter
- ✓ Inbyggd affärsberedskap som stöds av en pengarna-tillbaka-garanti
- ✓ Ett processdrivet ramverk för online-säkerhet för att klara svenska krav vad gäller integritet och hälsoinformation, och klara certifieringar som ISO 27001, SAS 70 Type II, SSAE16 och EU Safe Harbor.

Vi är Microsoft in Health.
www.microsoft.com/health

Om detta dokument

Informationen i det här dokumentet representerar Microsoft Corporations hållning i de här frågorna som den var vid publiceringstillfället. Eftersom Microsoft måste reagera på förändrade marknadsförhållanden ska det här dokumentet inte tolkas som något åtagande från Microsoft. Microsoft kan inte heller garantera att informationen stämmer efter publiceringsdatumet.

Detta White Paper publiceras endast i informationssyfte. MICROSOFT GER INGA GARANTIER, UTTRYCKLIGA, UNDERFÖRSTÅDDA ELLER LAGSTADGADE, VAD GÄLLER INFORMATIONEN I DET HÄR DOKUMENTET.