Exp 090604

2009-05-29
Beslut
Dnr LiU-2009-00857
1(15)

Informationssäkerhet vid Linköpings universitet

Inledning

Universitetsstyrelsen fastställde 2002-02-27 IT-strategi för Linköpings universitet. Där fastslås att tillämpningen av IT inom universitetet skall vara kostnadseffektiv, säker, driftsäker och pålitlig. Detta dokument tar sin utgångspunkt i detta.

Arbetet med informationssäkerhetsarbetet på LiU syftar till att säkerställa att universitetets IT-resurser har den tillgänglighet, tillförlitlighet och konfidentialitet som verksamheten behöver. För att åstadkomma detta räcker det inte med enskilda tekniska åtgärder. Informationssäkerhetsarbetet utgår från ledningsnivån och omfattar alla anställda och studenter. Informationssäkerhetsarbetet på LiU omfattar administrativ säkerhet och teknisk säkerhet i form av IT-säkerhetsarbete.

Mål

Informationssäkerhetsarbetet skall utgå från att universitetet skall utgöra en öppen miljö där institutioner och enheter har möjlighet att utforma sitt egna IT-stöd inom de gemensamma ramarna. Med hänsyn till den ständigt förändrade hotbilden mot system och information kan det vara nödvändigt att vidta åtgärder som i vissa fall begränsar öppenheten.

Informationssäkerhetsarbetet skall ha som mål att anställda och studenter skall kunna använda IT-resurser utan oönskade störningar och med hög grad av tillgänglighet, tillförlitlighet och konfidentialitet.

Organisation

Universitetsledningen har det övergripande ansvaret för informationssäkerheten inom universitetet medan respektive systemägare själv har ansvaret för säkerheten i egna system. Ledningsnivån utgörs i dessa frågor av universitetets administrative direktör, IT-direktören samt områdeschefen för LiU-IT. Arbetet på ledningsnivå i dessa frågor samordnas av IT-direktören som därmed även utgör universitetets IT-säkerhetssamordnare.

IT-säkerhetssamordnaren har det löpande ansvaret för såväl förebyggande arbete som implementering och uppföljning. Denne har också befogenhet att besluta om åtgärder såsom avstängning från nätet av IT-resurser som utgör ett hot mot säkerhet i datornät och datasystem.

Övervakning, loggning och utredning av intrång med mera uppdras (i särskild ordning) till en IT-säkerhetsgrupp (Incident Response Team, IRT). IT-säkerhetssamordnaren är beställare och följer arbetet i nära kontakt med utförarna.

IRT svarar för de kontakter med polis och övriga rättsvårdande myndigheter som föranleds av informationssäkerhetsarbetet. Universitets juristfunktion är här en stödjande funktion.

Inom varje institution/enhet är prefekten, enhetschefen eller motsvarande ansvarig för informationssäkerheten. Säkerhetsarbete kan utföras av anställda internt eller upphandlas. Vid varje institution och annan enhet skall finnas en kontaktperson som skall medverka i informations- och erfarenhetsutbyte i dessa frågor.

IT-säkerhetssamordnaren ansvarar för att årligen revidera och vid behov föreslå förändringar av LiUs policy för informationssäkerhet. Som stöd för denna verksamhet används det LiU-övergripande rådet för IT och infrastruktur.

Ansvar

a) Universitetsledningen

Universitetsledningen ansvarar för att fastställa policies, regler och delegationsordning inom informationssäkerhetsområdet som gäller för hela universitetet.

b) Administrative direktören

Den administrative direktören ansvarar för att rutiner och metoder finns för informationsspridning inom informationssäkerhetsområdet.

c) Prefekter och enhetschefer

Prefekter och enhetschefer är ansvariga för informationssäkerheten inom sin institution eller annan enhet. Prefekter och enhetschefer har möjlighet att delegera det operativa informationssäkerhetsarbetet.

Prefekter och enhetschefer ansvarar för att personalen får nödvändiga kunskaper för att IT-hjälpmedel skall kunna utnyttjas på ett säkert och effektivt sätt.

d) Systemägare

Varje systemägare ansvarar för informationssäkerheten i det egna systemet. Säkerhetsnivå och skyddsåtgärder skall fastställas utgående från bedömning av hotbilden och av konsekvenserna av störningar. Skyddsåtgärder skall väljas så att nyttan är rimlig i förhållande till kostnaderna för skyddet. Rutiner för förvaltning inklusive informationssäkerhetsarbete skall dokumenteras och uppdateras kontinuerligt.

e) Alla användare

Alla användare skall vara medvetna om informationssäkerhetsfrågornas betydelse och ha de kunskaper de behöver för att använda universitetets IT-resurser på ett säkert sätt.

Regler och riktlinjer

Universitetet är anslutet till SUNET (Swedish University Network) och är därmed skyldigt att följa SUNET:s regler (http://www.sunet.se/). Därutöver har följande lokala regler utarbetats för användningen av universitetets IT-resurser:

a) Användning

Var och en ansvarar för säkerhet i samband med sin egen datoranvändning. Lokala regler klargör hur universitetets allmänna IT-resurser får utnyttjas (återfinns i både svensk och engelsk version på http://regelverk.liu.se/innehft/ under fliken Lokala regelsamlingen/IT/Regler för IT användning vid LiU):

- Regler för studenters användning av dator-, nät- och systemresurser vid Linköpings universitet.
- Regler för anställdas användning av dator-, nät- och systemresurser vid Linköpings universitet
- Användning av dator-, nät- och systemresurser vid Linköpings universitet – ansvar, rättigheter och skyldigheter för systemadministratörer

Därutöver kan prefekt, enhetchef och systemägare utfärda regler för egna system och ansvarar då också för information om detta.

b) Drift av nät och servrar

Nät- och serverutrustning som ansluts till universitetets nät kan utgöra en säkerhetsrisk om installation, drift och underhåll inte sköts. Institutioner och andra enheter som driver egna system måste ha nödvändig kompetens. Särskilda regler finns för:

- Säkerhet för enskilda datorsystem
- Kryptering av datatrafik
- E-postservrar
- Identifiering av användare

c) Systemförvaltningsmodell

För LiU-gemensamma IT-system gäller att de ska förvaltas i enlighet med beslut dnr LiU 447/05-10.

d) Lokala resurser

Varje användare av IT-resurser bör känna trygghet att den egna informationen kan uppfylla krav på tillgänglighet, tillförlitlighet och konfidentialitet. Detta gäller såväl stationär utrustning på arbetsplatsen som bärbar utrustning. För detta ändamål finns fastställda regler för:

- Säkerhet för enskilda datorsystem
- Antivirus
- Säkerhetskopiering

e) Utbildning och information

IT-resurser blir allt viktigare verktyg inom universitetets verksamhet. Det är nödvändigt att anställda och studenter har tillgång till utbildning och information för åstadkommande av effektiv och säker IT-användning. Universitetet tillhandahåller utbildning för de vanligaste verktygen och det ankommer på prefekter och enhetschefer att motivera anställda att ta del av dessa liksom studenter bör uppmuntras att utnyttja de läromedel som tillhandahålls.

Systemägare kan föreskriva att användare måste ha genomgått viss utbildning.

Regler och viktig information bör finnas lätt tillgänglig via WWW och information om säkerhetshöjande åtgärder skall utarbetas och publiceras.

Upphandling, utveckling och införande av IT-system

Vid upphandling, utveckling och införande av IT-system och IT-tjänster skall reglerna i detta dokument följas. Eventuella avsteg skall godkännas av IT-säkerhetssamordnaren.

Konsulter och andra externa användare

När konsulter och andra externa användare ges tillgång till universitetets IT-resurser skall universitetet genom avtal försäkra sig om att användningen sker i enlighet med universitetets regler och med upprätthållande av god säkerhet.

Rapportering och uppföljning

Informationssäkerhet är ett gemensamt ansvar och var och en har därför skyldighet att rapportera iakttagna risker och incidenter (i enlighet med utfärdade regler för IT-användning). Nya hot och risker identifieras ständigt varför det är nödvändigt att fortlöpande aktivt arbeta för säkerheten. IT-säkerhetssamordnaren har ansvar för att informationssäkerhetsarbetet inom institutioner och andra enheter följs upp och att erfarenhetsutbyte sker.

Intrång och andra incidenter skall, utan dröjsmål, rapporteras till IRT, som också kan bistå vid utredning och eventuella åtgärder. Vid gemensamma akuta IT-säkerhetsproblem förväntas alla institutioner och andra enheter medverka till skyndsam lösning.

Detta beslut ersätter det tidigare beslutet LiU 1686/02-14 och skall publiceras i LiUs regelverk. Beslutet innehåller en huvuddel samt 9 bilagor med åtgärder för ökad IT-säkerhet.

I detta ärende har Rektor Mille Millnert beslutat efter föredragning av IT-direktör Joakim Nejdeby.

Mille Millnert

Joakim Nejdeby

Kopia till
Universitetsledningen
Fakulteterna
Institutionerna
Universitetsbiblioteket
Universitetsförvaltningen

LiU-IT
NSC
Studentkårerna
Internrevisionen
De lokala fackliga organisationerna

Bilaga 1.
Åtgärder för IT-säkerhet: Säkerhet för enskilda datorsystem

Varje dator som är ansluten till Linköpings universitets nätverk har betydelse för IT-säkerheten i stort. Felaktigt installerade datorer och datorer som inte uppdaterats med säkerhetsuppdateringar från programvaruleverantörer utgör ett hot mot resten av nätverket. Detta gäller serversystem men också enskilda persondatorer, vilket innebär att kraven ökar på en aktiv förvaltning av samtliga datorsystem.
Även annan utrustning, såsom skrivare, scanners, videokonferenssystem, avancerade mobiltelefoner med mera, som ansluts till nätverket kan påverka säkerheten. Det som sägs nedan om datorer gäller i tillämpliga delar även sådan utrustning.
De som sköter datorer och annan utrustning måste därför ha kompetens för detta och måste kontinuerligt hålla sig informerade om hotbilder och åtgärder mot dessa.

Härmed beslutas:

- Vid inköp av datorer och programvara skall hänsyn alltid tas till IT-säkerhetsaspekter i god tid.
- Datorer på universitetets nätverk samt programvaran på dessa skall installeras på ett sådant sätt att onödiga risker inte uppstår.
- Datorerna skall kontinuerligt uppdateras med de säkerhetsuppdateringar som leverantörer av operativsystem, tillämpningar med mera gör tillgängliga.
- Programvaror och tjänster som inte används skall stängas av. Detta är särskilt viktigt för server-datorer.
- Medföljande brandväggsprogramvara på datorerna bör användas för att minska riskerna för otillbörlig åtkomst.
- Utrustning och programvara som inte hålls uppdaterad och säker skall kopplas bort från universitets nätverk.

Bilaga 2.
Åtgärder för IT-säkerhet: Lösenordshantering för användare

En mycket viktig del i IT-säkerheten är att alla användare har bra lösenord som byts regelbundet. Vid förlust av ett lösenord kan tillförlitligheten och konfidentialiteten av informationen i ett LiU övergripande system allvarligt äventyras. Det finns system med högre säkerhetskrav som därför kan ha ytterligare krav som bestäms av respektive systemägare.

Olika lösenord

- Du bör inte använda samma lösenord till allting.
- Använd aldrig samma lösenord på universitetets system som du använder till webbtjänster på Internet. Använd aldrig samma lösenord på viktiga system med höga säkerhetskrav och mindre viktiga system.
- Det är även olämpligt att återanvända gamla lösenord. Hitta hellre på ett helt nytt för nya syften.

Bra lösenord

- Välj ett långt lösenord (minst 8 tecken, gärna längre).
- Använd en blandning av stora och små bokstäver, siffror och andra tecken (som "!%&").
- I system som tillåter ordentligt långa lösenord kan det vara ett bra alternativ att använda en hel fras (passphrase) bestående av många ord istället för ett kort lösenord. Frasen måste vara lika svårgissad som ett vanligt lösenord.
- Ytterligare ett alternativ är att hitta på en hel fras som ovan och sedan ta initialbokstäverna i varje ord, samt krydda med lite siffror och/eller specialtecken.
- Använd enbart a-z och A-Z bland bokstäverna, eftersom vissa system har problem med "svenska tecken" (ääöÅÄÖ) med mera.

Dåliga lösenord

- Vissa system tillåter tyvärr inte lösenord över en viss längd (till exempel åtta tecken). Det finns en risk att vissa system bara ser till början av ett långt lösenord. Det gäller då att redan denna första del är bra nog.
- Undvik teckenkombinationer som ligger i lättgissade mönster på tangentbordet (till exempel "qwerty", "asdfgh", "1234567890") eller är ordnade på annat enkelt sätt ("abcdefghijk").
- Undvik ord eller namn. Dessa finns nämligen med i de ordlistor som används av de som försöker gissa lösenord.
- Undvik lösenord som kan gissas om man vet något om dig (till exempel användarnamn, eget namn, namn på anhöriga, namn på husdjur, registreringsnummer, telefonnummer, personnummer).
- Lägg inte bara till en siffra först eller sist i ett i övrigt lättgissat lösenord.
- Byt inte bara ut tecken mot "liknande" (till exempel "gr33n" istället för "green") i ett i övrigt lättgissat lösenord.

Byta lösenord

Lösenord skall bytas direkt om det finns misstanke om att någon obehörig fått tillgång till det. Detta gäller också om din dator där du använt lösenordet blivit stulen. Diskutera också det som hänt med den IT-säkerhetsansvarige på din institution eller enhet.

Lösenord bör bytas ibland för att minska risken att lösenord som stulits eller gissats kan fortsätta att användas, även om inga konkreta misstankar finns. I det flesta system som inte har särskilda krav är det lämpligt att byta en gång per år.

Avslöja lösenord

Ingen person skall fråga dig efter ditt lösenord (via telefon, epost eller på annat sätt). Detta gäller även systempersonal på universitetet. Om detta inträffar ändå: vägra att uppge ditt lösenord och rapportera genast händelsen till den IT-säkerhetsansvarige på din institution eller enhet.

Skicka aldrig lösenord osäkert via e-post, chat eller liknande tjänster. Det finns risk att det hamnar hos fel mottagare eller att någon snappar upp det på vägen.

Bilaga 3.
Åtgärder för IT-säkerhet: Kryptering av datatrafik

Varje systemägare ansvarar för säkerheten i egna system. Säkerhetsnivå och skyddsåtgärder skall fastställas utgående från bedömning av hotbilden och av konsekvenserna av störningar. Skyddsåtgärder skall väljas så att nyttan är rimlig i förhållande till kostnaderna för skyddet.

Trafik i datornätverk kan avlyssnas med mycket enkla medel, t.ex. finns allmänt tillgänglig programvara som explicit söker efter loginnamn/lösenord, vilket medför att okrypterade lösenord över datornätverk i princip kan likställas med att systemet i fråga är helt oskyddat.

Det finns flera tekniska möjligheter för att kryptera datatrafik och IT-säkerhetsamordnaren erbjuder råd vid behov.

Mot denna bakgrund fastställs följande:

1. Inloggningsinformation (lösenord och liknande) skall alltid överföras krypterat.
2. Skyddsvärda data bör alltid överföras krypterat. Vad som är skyddsvärt måste bedömas av den enskilde systemägaren. Några exempel är:
    - Sekretessbelagda data
    - Personuppgifter
    - Ännu ej given tentamen
    - Data i samband med företagssamarbete

Bilaga 4.
Åtgärder för IT-säkerhet: Identifiering av användare

För att upprätthålla IT-säkerheten har universitetet ett behov av att kunna identifiera vem som använder datorer och nät. Det finns också ett behov av att kunna spåra enskilda datorer i samband med intrång, virusangrepp och liknande.

I "Regler för tillåten användning av SUNET" finns dessutom följande bestämmelse:
"En organisation som använder SUNET via publika terminaler skall tillse att det finns ett system för identifiering av användarna av de publika terminalerna."

Därför gäller:

- Nätanslutna datorer skall ha inloggningssystem som kräver inloggning med personligt konto.
- Trådlöst nätverk och publika nätverksuttag skall ha system som verifierar användaridentitet innan åtkomst ges till nätverket.
- Nätverk skall övervakas så att datorer kan spåras till det uttag de är eller varit inkopplade i.

Bilaga 5.
Åtgärder för IT-säkerhet: Antivirus

Virus och elak kod (datorprogram som installeras utan samtycke i skadligt syfte) medför risker som måste hanteras. Därför beslutas:

- Antivirus skall finnas installerat i alla nätanslutna virushotade datormiljöer
- Antivirus skall uppdateras automatiskt och ofta (minst dagligen om nätanslutning finns).

För att hantera risken med skadlig programvara gäller följande:

- Datorer som misstänks vara infekterade med elak kod skall kopplas bort från nätverket och kontrolleras med ett uppdaterat antivirusprogram.
- Om en dator visar sig vara infekterad med elak kod skall detta omgående rapporteras till Incident Response Team (IRT).

Bilaga 6.
Åtgärder för IT-säkerhet: Säkerhetskopiering

En mycket stor del av universitetets information finns lagrad på olika typer av datamedia. Förlust eller skada på informationen genom tekniska problem, stöld av utrustning eller andra oönskade händelser kan medföra stora skador för universitetet, både ekonomiskt och arbetsmässigt.

För att säkerställa att för universitetet väsentlig information inte går förlorad beslutas härmed att:

- Säkerhetskopiering skall ske av väsentlig information, såväl på servrar som arbetsstationer
- Säkerhetskopiorna skall förvaras väl skyddade från stöld, skada och obehörig åtkomst.
- Det skall finnas kopior "off-line" (ej åtkomliga och modifierbara utan fysisk åtkomst till media) av viktig information.
- Skriftliga rutiner för säkerhetskopiering skall finnas inom samtliga institutioner och andra enheter

För användare rekommenderas att man använder fillagertjänst med inbyggd säkerhetskopiering för att uppfylla ovanstående krav.

Bilaga 7.
Åtgärder för IT-säkerhet: Radering av hårddiskar och andra datamedia

Det finns många skäl att se till att hårddiskar och andra datamedia inte lämnas vidare utan att innehållet på dem raderats eller på annat sätt gjorts oläsligt.

På hårddiskar från datorer är det troligt att det finns lösenord, inställningsfiler med mera, som inte får spridas till obehöriga, därför att det kan äventyra IT-säkerheten. En uppenbar anledning är också att det kan finnas känsliga verksamhetsuppgifter lagrade, som inte får bli offentliga. Det är också möjligt att det på hårddiskar finns program installerade, vars licensvillkor inte tillåter att de används utanför universitetets verksamhet.

Därför beslutas:

- Hårddiskar skall raderas (med programvara som skriver över innehållet ett flertal gånger med olika datamönster) innan de överlåtes till utomstående eller kasseras.
- Om så inte kan ske skall de förstöras fysiskt på ett sätt som omöjliggör återläsning av informationen.
- Ovanstående kan utföras av personal på universitetet eller genom skriftligt avtal med företag som tar hand om utrustningen för skrotning.
- Samma regler gäller för andra datamedia (USB-minnen, CD/DVD-skivor, band, disketter med mera) om det kan antas finnas känslig information på dem.

Innehåller datamediet allmänna handlingar kan det vara fråga om gallring (förstörelse) i lagens mening. Gallring kräver att det finns beslut om att uppgifterna kan tas bort.

Bilaga 8.
Åtgärder för IT-säkerhet: E-postservrar

E-post är ett viktigt arbetsredskap på universitetet. För att detta ska fungera måste eposten skyddas från virus (och annan elak kod) och spam.

Därför beslutas:

- E-postservrar som används av användare med virushotad datormiljö skall ha antivirusfiltrering av e-posten.
- E-postservrar som är åtkomliga utifrån Internet skall ha fungerande reläskydd som ser till att de inte kan missbrukas för spamskickande.
- E-postservrar som är åtkomliga utifrån Internet skall använda aktuella spamskyddstekniker för att begränsa inkommande spam.

IT-säkerhetssamordnaren (eller de som uppgiften delegerats till) har rätt att bestämma vilka e-postservrar som får vara åtkomliga utifrån Internet.

Bilaga 9.
Åtgärder för IT-säkerhet: VPN-användning

Tillträde till universitets IT-resurser genom uppkoppling via VPN (Virtual Private Network) innebär att den enskilde användaren själv måste ansvara för att säkerheten upprätthålls.

Följande gäller för all VPN-användning:

- VPN-kontot är personligt och får inte upplåtas till annan person.
- Datorn måste uppfylla kraven i "Åtgärder för IT-säkerhet: Antivirus".
- Datorn skall hållas uppdaterad vad avser säkerhetsuppdateringar och liknande.
- Den VPN-programvara som universitetet tillhandahåller eller anvisar skall användas för uppkopplingen.
- VPN-anslutningen bör kopplas ned när den inte behövs .
- Datorn måste hållas säker även under de perioder då den inte är uppkopplad via VPN.
- Systemägare kan besluta att ytterligare villkor ska gälla för tillträde till särskilt känsliga system.