Incidenthantering för IT-incidenter

Bakgrund

Oväntade händelser kan ha effekt på arbetet vid högskolan och i värsta fall orsaka stora ekonomiska och förtroendemässiga förluster. Det är därför viktigt att få en god överblick över vilka incidenter som inträffar för att på detta sätt tidigt kunna spåra mönster och trender så att nödvändiga åtgärder kan sättas in utan dröjsmål. En god kontroll över högskolans incidenter möjliggör också en bättre planering och prioritering av åtgärder och gör att vi har möjlighet att inte upprepa tidigare misstag. En väl utbyggd och fungerande incidenthantering är också en förutsättning för den obligatoriska rapportering av IT-incidenter som gäller enligt MSB's föreskrifter i enlighet med SFS 2015:1052.

Definitioner

Brukare – Brukare är den som använder någon av högskolans IT-tjänster eller IT-enheter. Brukarens rättigheter och skyldigheter regleras i dokumentet ”Användarens rättigheter och skyldigheter”.

IT-incident - En oönskad och oplanerad it-relaterad händelse som kan påverka säkerheten i organisationens eller samhällets informationshantering och som kan innebära en störning i organisationens förmåga att bedriva sin verksamhet.

IRT-grupp – IRT-gruppen består av högskolans IT-chef, jurist samt Informationssäkerhetsansvarig. Gruppens arbete regleras i dokumentet ”Ansvar, befogenheter och skyldigheter för medlem i incidentgrupp”

IT-tekniker – **I**T-tekniker är den som är anställd vid MAH som IT-tekniker eller innehar motsvarande befattning. IT-teknikerns arbete regleras i dokumentet ”Ansvar, befogenheter och skyldigheter för IT-tekniker.

Systemägare – Systemägaren är den som är utsedd av rektor att ha det administrativa ansvaret för ett IT-system.

Ansvar

- Systemägaren är ansvarig för att systemet har ett adekvat skydd för att undvika IT-incidenter i den utsträckning som är nödvändig mot bakgrund av systemets riskvärden.
- IT-avdelningen är ansvarig för att aktivt bistå systemägaren i säkerhetsarbetet med systemet.
- Brukaren är ansvarig för att rapportera misstänkta IT-incidenter till IT-service och skall följa de riktlinjer och säkerhetsföreskrifter som finns för systemet.
- Den IT-tekniker eller motsvarande som hanterar en IT-incident är ansvarig för att arbetet utförs och rapporteras i enlighet med detta dokument och andra regler som följer av högskolans informations- och IT-säkerhetspolicy.
- IRT-gruppen är ansvarig för att leda arbetet vid allvarliga IT-incidenter och kan medge avsteg från fastställda rutiner i nödvändiga fall.

Arbetets utförande

IT-Incidenter kan inträffa på en rad olika sätt och områden. Det gemensamma är att det handlar om oväntade och oönskade händelser som har en risk för att åstadkomma skada på högskolans arbete. Då en IT-incident upptäcks är det därför viktigt att den snabbt behandlas korrekt för att minska risken för följdskador. Åtgärder skall därför sättas in enligt följande prioritetsordning:

1. Stoppa omedelbart, så långt det är tekniskt möjligt, de negativa effekterna av incidenten.
2. Kontrollera och säkra dokumentation över vad som har inträffat.
3. Återställ funktionen.
4. Utred och rapportera incidenten.

Arbetet skall utföras i enlighet med ovanstående punkter och skall rapporteras enligt nedan. Avsteg från arbetsgången, exempelvis vad gäller krav på omedelbart stopp, kan medges av IRT-gruppen och skall meddelas skriftligt.

Arbetet skall övergripande följa IT-incidentrapporteringsprocessen och för det interna arbetet inom ITI och ITS sker detta enligt respektive enhets interna föreskrifter.

Rapportering

För att förebygga problem och begränsa verkningarna av inträffade IT-incidenter är det av stor vikt att högskolan har en korrekt och relevant rapportering. Ett bra underlag är nödvändigt för att prioriteringar skall kunna göras effektivt kring val av verktyg och metoder för det förebyggande arbetet. Detta gäller både för det dagliga arbetet såväl som för högskolans strategiska planering. Varje IT-incident skall därför rapporteras av den åtgärdande IT-teknikern, eller motsvarande, i Service Manager och klassificeras enligt Incidentklassificering nedan. Varje rapport skall även innehålla uppgift om:

- tidpunkt då incidenten upptäcktes
- tidpunkt då incidenten inträffade
- kort beskrivning av händelsen
- vilka skador som har åsamkats högskolan
- om förlust av information har skett
- om sekretessbelagd information har läckt ut
- om information har förvanskats

Rapportering till IRT sker för samtliga incidenter som gäller fullbordat intrång eller virusinfektion på server som ingår i något av högskolans aktiva system, samtliga tillfällen då högskolans utrustning används för att attackera system utanför högskolan och för samtliga fall, oavsett typ av incident, då prioriteten bedöms till 1.

Rapportering till MSB i enlighet med föreskrifterna för statliga myndigheters rapportering av IT-incidenter och görs av informationssäkerhetsansvarig eller av denne utsedd person. Ansvarig för rapporteringen är Informationssäkerhetsansvarig.

Incidentklassificering

För att korrekt kunna bedöma vilka resurser som kan motiveras för att hantera en incident är det nödvändigt att korrekt klassificera incidenten. Incidenter skall därför klassificeras i enlighet med

nedanstående tabell samt högskolans tjänstekatalog.
I klassificeringen ingår, förutom en bedömning av vilken tjänst och typ av IT-incident det rör sig om, också en bedömning av vilken prioritet åtgärderna har. Bedömningen görs från 1 till 5 och sätts så att prioritet 1 tilldelas händelser som innebär eller kunde ha inneburit mycket allvarliga konsekvenser för högskolans verksamhet ner till prioritet 5 för händelser som har inga eller försumbara konsekvenser. Tabellen nedan innehåller normalvärden som stöd för konsekvensbedömningarna för de olika klassificeringarna men omständigheterna kan vara sådana att den korrekta bedömningen kan ligga utanför detta intervall.

Typ av incident	Hantering	Rapportering	Prioritet (1-5)
Intrångsförsök	Hanteras av ITI	ja	(Normalt 3-5)
Lyckat intrång eller virusinfektion på wst (Intrång/virus på wst)	Hanteras av ITS	ja	(Normalt 3-4)
Lyckat intrång eller virusinfektion på srv (Intrång/virus på srv)	Hanteras av ITI	Ja + utredning + rapport till IRT	1
Högskolans utrustning används i mot omvärlden (Attack mot omvärlden)	Hanteras av ITS och ITI	Ja + utredning + rapport till IRT	1
Hårdvarufel på wst	Hanteras av ITS	ja	(Normalt 3-4)
Hårdvarufel på srv	Hanteras av ITI	Ja + utredning	(Normalt 3-5)
Hårdvarufel på övrig IT-utrustning (Hårdvarufel övrigt)	Hanteras av ITI eller ITS	ja	(Normalt 3-5)
Administrativt fel (avtalsbrott, bedrägeri, upphovsrättsbrott etc) (Administrativt fel)	Hanteras av SLM eller annan avtalsansvarig	ja	(Normalt 3-4)
Stöld	Hanteras av ITS	ja	(Normalt 2-4)
Övrigt	Hanteras av ITI eller ITS beroende på felets art	Ja, möjligen rapport till IRT samt utredning beroende på felets art och omfattning	

Verktyg

All incidentrapportering skall ske i Service Manager enligt de regler för rapportering och registrering som gäller för ITS respektive ITI.

Uppföljning

All incidentrapportering skall finnas tillgänglig för IT-avdelningen och IRT-gruppen. Enhetscheferna för ITI och ITS ansvarar för att arbetet inom respektive enhet följs upp. En årlig sammanställning av inträffade incidenter skall göras av informations- och IT-säkerhetsansvarig och redovisas tillsammans med övrigt arbete inom högskolans ledningssystem för informationssäkerhet.

IT-incidentrapporteringsprocessen