HÖGSKOLAN
I HALMSTAD

Rutinbeskrivning: Incidenthantering med avseende på informationssäkerhet vid Högskolan i Halmstad

Fastställd av IT-chef 2019-01-22, dnr I 2018/62

Bakgrund

Andra myndigheter ställer krav på Högskolans incidenthantering, både vad gäller informationssäkerhet i stort, och specifikt vad gäller IT-incidenter och personuppgiftsincidenter.

Med informationssäkerhetsincident menas i detta fall en oönskad och oplanerad händelse som kan påverka säkerheten i Högskolans eller samhällets informationshantering eller som kan innebära en störning i Högskolans förmåga att bedriva sin verksamhet. Orsaken till incidenten kan exempelvis vara bristande kompetens, mänskliga misstag, tekniska avbrott eller naturhändelser. Av detta följer att IT-incidenter har en koppling till Högskolans IT-utrustning, data- eller telekommunikation, och att personuppgiftsincidenter endast omfattar de incidenter som (kopplat till personuppgifterna) medför risker för enskildas fri- och rättigheter.

Åtgärder

När en incident upptäcks ska i första hand risken för skada minimeras. Därefter sker rapportering. Är incidenten sådan att det misstänks att andra myndigheters incidenthanteringsorganisationer kan dra nytta av rapportering ska rapporteringen prioriteras.

Rapportering av incidenter som omfattar IT-stödet rapporteras till direkt till IT-avdelningen via Helpdesk eller annan metod.

Persondataincidenter hanteras enligt särskild ordning (dnr L 2018/83).

Intern rapportering

Alla incidenter av typerna som specificeras nedan rapporteras via epost till IT-handläggaren, som gör en bedömning ifall incidenten är sådan att den även ska rapporteras vidare till Myndigheten för Skydd och Beredskap (MSB) eller om en polisanmälan ska göras. De incidenter som beskrivs i punkterna b), c), g), j) och l) ska alltid rapporteras till MSB.

a) Oplanerade stopp i IT-system som påverkar merparten av studenterna, antingen i 4 timmar eller mer, eller återkommande
b) Oplanerade stopp i IT-system som påverkar viktiga delar av Högskolans kommunikation med omvärlden antingen i 4 timmar eller mer, eller återkommande
c) Känsliga, eller stora mängder, personuppgifter som läckts hittas på Internet (inte sådana som HH lämnat ut enligt offentlighetsprincipen)
d) Upptäckt skadlig kod
e) Missbruk av inloggningsuppgifter för konto med högre behörighet
f) Otillåtet tillträde till server/nätutrustning etc upptäcks
g) Nya phishing-meddelanden som innehåller Högskolan i Halmstads logga/inloggningsrutor etc
h) Anställd raderar/ändrar medvetet data i syfte att förstöra data (t.ex. i vredesmod)
i) Högskolans konton i sociala medier har använts av obehörig som spridit falsk information

j) hh.se (eller andra domäner som Högskolan äger) kapas
k) Utrustning med okrypterad och känslig information försvinner
l) Högskolans internetkoppling bryts oavsiktligt, i en timme eller mer
m) Förlorad redundans i central utrustning under längre tid än beräknat
n) Inrapporterade persondataincidenter
o) Dataförlust av tekniska orsaker

Rapporten till IT-handläggaren ska innehålla följande:

1. Benämning på incidenten
2. Är incidenten konstaterad eller misstänkt?
3. Är incidenten pågående, avbruten/hanterad eller avslutad?
4. Vad har hänt?
5. När upptäcktes det? (datum, klockslag; exakt tid eller uppskattad tid)
6. När inträffade det? (datum, klockslag; exakt tid eller uppskattad tid)
7. Berörd utrustning?
8. Berörda användare?
9. Är någon extern part berörd?
10. Konsekvenser?
11. Akuta åtgärder (för att minska konsekvenser för HH resp. användare)?
12. Hur har berörda användare (som ej rapporterat felet) informerats?
13. Vilken kategori hör incidenten till?
    a) Störning i mjuk- eller hårdvara
    b) störning i driftmiljö
    c) informationsförlust eller informationsläckage
    d) informationsförvanskning
    e) hindrad tillgång till information
    f) säkerhetsbrist i en produkt
    g) angrepp
    h) handhavandefel
    i) oönskad eller oplanerad störning i kritisk infrastruktur, eller
    j) annan plötslig oförutsedd händelse som lett till skada.
14. Hur omfattande var störningen för Högskolans verksamhetskritiska tjänster? (begränsad, stor, mycket stor, okänd)
15. Finns behov av återställning? Eventuell planerad tidsåtgång för återställning
16. Långsiktiga åtgärder (för att förhindra upprepning)?
17. Övrig information om incidenten (t.ex. ärendenummer i Helpdesk)

En gång per år lämnas en rapport till Högskolestyrelsen som bland annat innehåller information om de informationssäkerhetsincidenter som inträffat under året (enligt Rutinbeskrivning: Granskning och uppföljning av informationssäkerheten, dnr I 2018/64).

Extern rapportering

IT-säkerhetsincidenter

Inträffar en IT-säkerhetsincident som allvarligt kan påverka säkerheten för Högskolans informationshantering ska rapport skickas till MSB inom 24 timmar från att den kommit IT-handläggaren eller informationssäkerhetsansvarig till känna. Rapportering ska ske enligt MSB:s instruktioner.