Hackad, läckt eller bara fel mottagare?
Om hantering av personuppgiftsincidenter på SLU

Malin Johansson, Jurist, Ledningskansliet

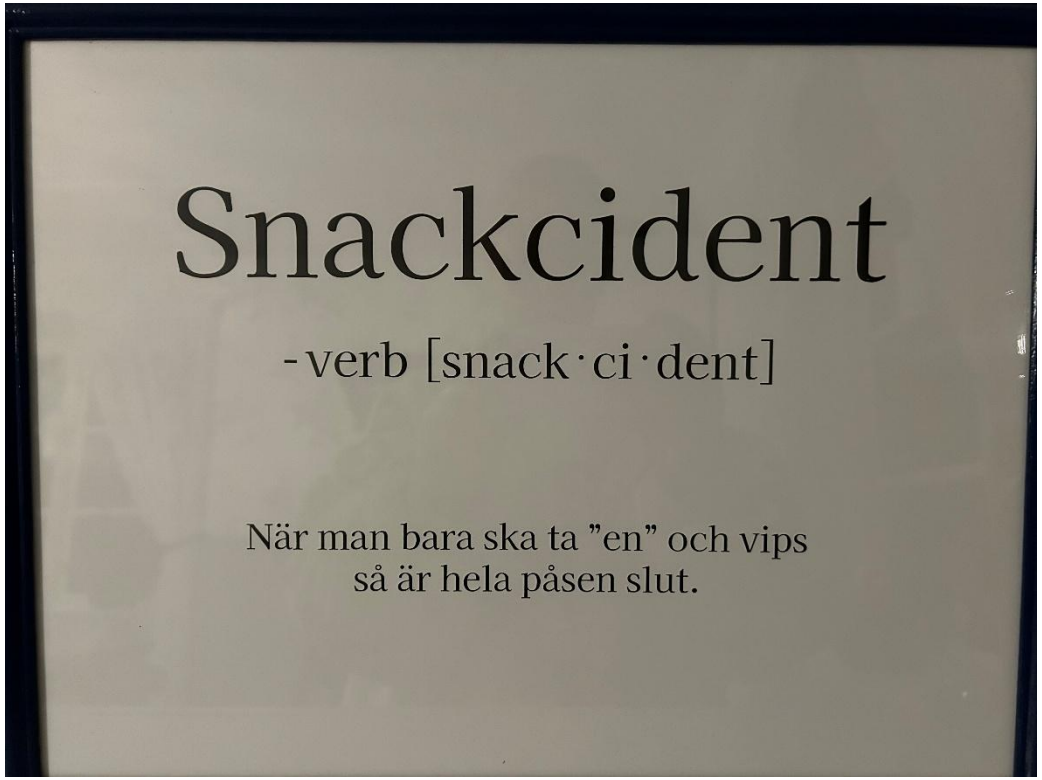
Finns många olika typer av incidenter

Informationssäkerhetsincident

IT-incident

Arbetsmiljöincident

Personuppgiftsincident



Definition

Artikel 4
12. **personuppgiftsincident:** en säkerhetsincident som leder till oavsiktlig eller olaglig **förstöring**, **förlust** eller **ändring** eller till **obehörigt röjande** av eller **obehörig åtkomst** till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,



Vad är behandling av personuppgifter?

Personuppgifter =

En personuppgift är en uppgift som indirekt eller direkt identifierar någon / kan kopplas till en (fysisk) person.

Behandling =

Behandling är allt man kan göra med personuppgifter genom en enskild åtgärd eller kombination av åtgärder.

Stulna eller borttappade enheter

- SLU datorer, telefoner, USB-minnen med mera som förloras på något sätt.
- Vanligt förekommande. Ex.
  - Glömt dator på flygplan
  - Tappat bort telefon på buss
  - Dator försvunnit från låst kontor
- Kom ihåg att anmäla det som en incident!



Skickat e-post utan hemlig kopia eller fel mottagare

- Grupp av kunder eller forskningsdeltagare får information utskickad till sig.
- Alla mottagare i *till-fältet* innebär att e-postadresserna avslöjas för de andra deltagarna.
- Obehörigt röjande.
- Skickar e-post innehållande personuppgifter eller bilaga innehållande personuppgifter fel.
- Om enda personuppgiften är din signatur kan det bortses från.
- Obehörigt röjande.
- Tips: om du råkar skicka fel skriv till personen direkt och be denne radera e-posten.

Behörighetsinställningar

- Att man jobbar vid SLU betyder inte att man har rätt att se allt.
- Felaktiga eller för breda behörighetsinställningar kan vara en personuppgiftsincident.
- Obehörigt röjande.
- Viktigt att arbeta med löpande.



Bug i planerat underhåll blev incident

- Planerat underhåll i SLU:s nätverk för att installera uppdragerad utrustning.
- Felsökning efter arbetet visade att flera system inte kom upp igen vilket åtgärder sattes in för.
- Måndag morgon inkom flera anmälningar till IT om vissa system som inte fungerade och filer som inte kunde kommas åt.
- Visade sig vara en bug i utrustningen som installerades.
- Tillgänglighetsincident.



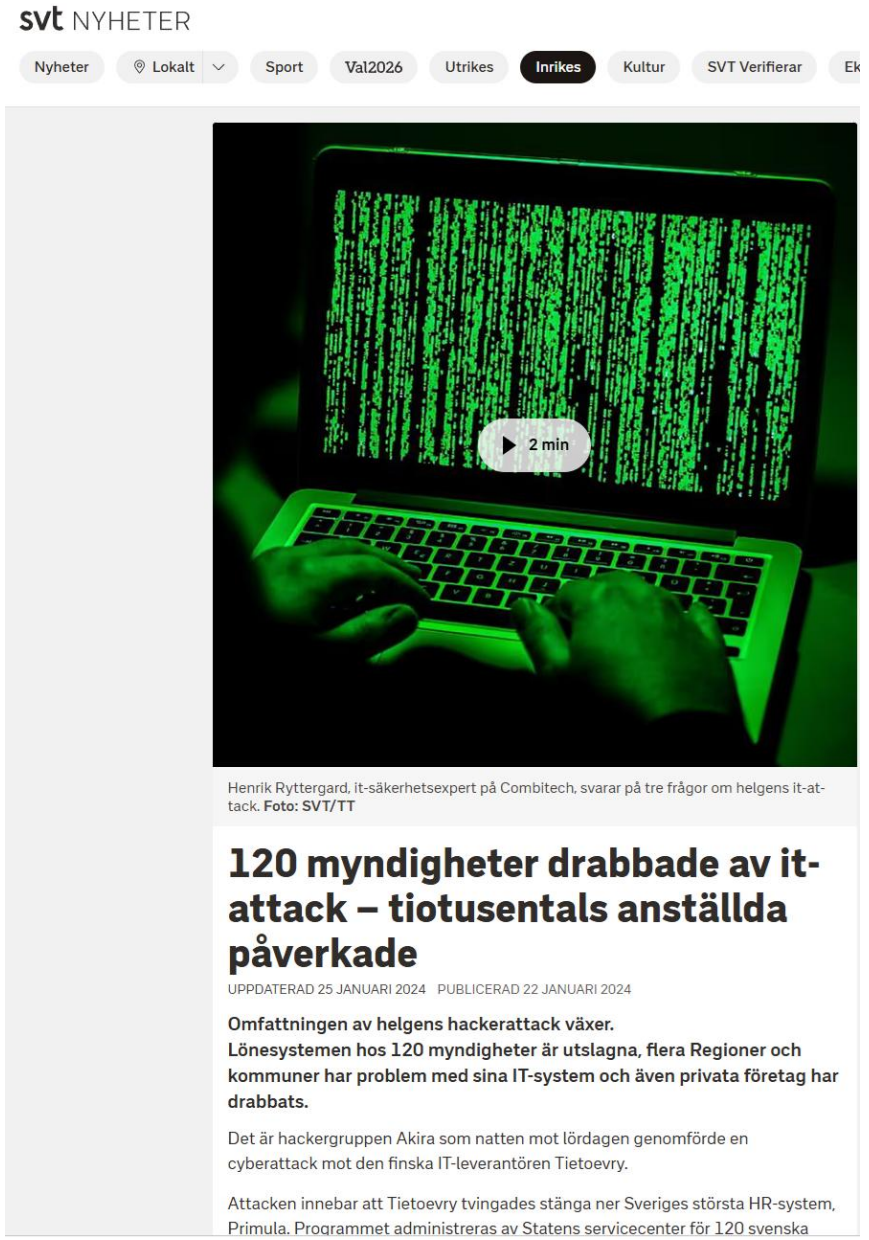
@slu.se svartlistad hos Microsoft

- Skickades ut massor a e-post från ett hackat studentkonto vilket ledde till att domänen @slu.se klassades som spam.
- Microsoft svartlistade domänen.
- Konsekvensen blev att SLU inte kunde skicka e-post externt.
- Tillgänglighetsincident – kunde inte utföra serviceskyldighet.



Ransomeware attack mot personuppgiftbiträde

- TietoEvry utsattes för ransomewareattack, vilket ledde till att system stängdes ned.
- Konsekvensen att SLU inte kunde komma åt Primula eller BeSched.
- Prioritet under incidenten – hur uppgifter som schemaläggning, lönekörning med mera skulle lösas.
- Tillgänglighetsincident.



120 myndigheter drabbade av it-attack – tiotusentals anställda påverkade | SVT Nyheter

Miljödata-läckan

- Leverantören av Adato blev utsatt för cyberangrepp och data blev stulen.
- Datan publicerades på Darknet.
- Obehörigt röjande.
- IMY har konstaterat att Miljödata inte hade vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå.



Upsala Nya Tidning.

Senaste nytt

CYBERANGREPP

Dataintrånget vid SLU drabbar anställda 16 år tillbaka i tiden

Publicerad 17 september 2025, kl 14.56

Dela

Sveriges lantbruksuniversitet, SLU, har lokaler vid Ultuna strax söder om Uppsala.
Foto: Staffan Claesson

I slutet av augusti utsattes SLU:s systemleverantör Miljödata för ett cyberangrepp. Uppgifter har läckt ut för 12 300 personer som är eller varit anställda på Uppsalabaserade SLU, Sveriges lantbruksuniversitet.

Personuppgifter för 12 300 personer vid SLU har läckt ut

Canvas incidenten

- Leverantören av Canvas fick intrång och data stulen.
- Stort antal påverkade på grund av att vi inte arkiverat och gallrat.
- Obehörigt röjande och tillgänglighetsincident genom att SLU valde att stänga ned Canvas under en viss.



Upsala Nya Tidning.

Senaste nytt

HACKERATTACK MOT CANVAS

SLU: Vi kan stänga ner sidan

Publicerad 8 maj 2026, kl 12.40

Dela

SLU ligger i Ultuna i Uppsala. Foto: Staffan Claesson

Innebär det risker att låta studenter ha tillgång till läroplattformen Canvas när den är under en hackerattack? Det är en fråga SLU vill ha svar på – som överväger att själva stänga ner sidan.

SLU överväger att stänga ner Canvas efter attack

Kan SLU få påföljder av incidenter

- Sanktionsavgifter
- Skadestånd
- Tillsyn kan leda till förbud eller föreläggande
- Förtroende- och varumärkesskada



Förebyggande åtgärder

- Vara noga med att kravställa till leverantörer
  - SLU:s kravkatalog för informations- och it-säkerhetskrav
- Se till att ha personuppgiftsbiträdesavtal när externa behandlar våra personuppgifter
  - Rekommenderas att dataskydd@slu.se är ingångskontakt för personuppgiftsincidenter
- Samla inte in eller spara onödig information.
- Arkivera!
- Kontinuitetsplanera.
- Ta dig tid att ta en extra titt.
- Kom ihåg att vi är mänskliga – misstag sker.

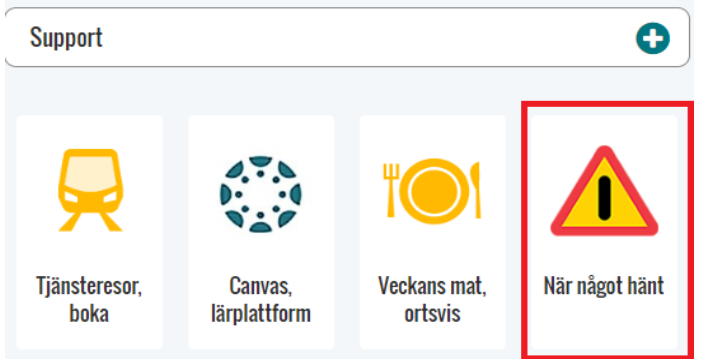


Dokumentera incidenter

- Personuppgiftsincidenter ska alltid dokumenteras internt.
- Om incidenten medför risk för registrerads fri- och rättigheter ska den anmälas till Integritetskyddsmyndigheten inom 72 timmar.



Vad du behöver göra?



- Om du upptäcker en incident rapportera den internt så snart som möjligt.
- Nuläge: IA-systemet
  - Kort beskrivning av vad som hänt, vad du gjort sedan upptäckt och vilka uppgifter som är påverkade
- På gång: ny enkät för informationssäkerhets- och personuppgiftsincidenter
  - Mer användarvänligt än IA-systemet
  - Frågar bara om det som behövs för att vi ska kunna göra en första bedömning

Framtidsspaning – incidenter kommer att öka

Open AI stäms efter intrånget mot Hugging Face

Nyhet

30 sep. 2026 • 1 min

Open AI har nu stämts efter att företagets AI-agenter i juli bröt sig ur sin testmiljö och gjorde ett intrång mot AI-plattformen Hugging Face. Bakom stämningen står den ideella organisationen Legal Advocates for Safe Science and Technology (LASST), rapporterar **CNBC**.

Butikskylar och frysar hackade – flera butiker drabbade

UPPDATERAD 3 NOVEMBER 2026 PUBLICERAD 2 NOVEMBER 2026

Flera Ica-butiker har fått sina frysar och kylar hackade. Även Coop-butiker har drabbats.

Home › Cyber Security

Massive Password Stealing Attack Targeting Microsoft 365 Users With 81 Million Login Attempts

Att ta med dig från idag

- Om du upptäcker en personuppgiftsincident rapportera den så snart som möjligt. Det är förväntat och naturligt att de inträffar.
- Fundera på och diskutera om det finns saker du och dina kollegor kan göra för att förebygga att en incident inträffar.
- Vi finns där och stöttar om en incident inträffar.



Frågor?



Tack för uppmärksamheten!

KONTAKTUPPGIFTER
Malin Johansson, jurist/legal counsel
018-67 28 48, malin.a.johansson@slu.se

Vid frågor om GDPR/dataskydd kontakta oss gärna på e-post dataskydd@slu.se

På internt.slu.se/dataskydd kan du hitta information om dataskyddsfrågor och även mallar

Om du har feedback gällande temaveckan skicka den gärna till malin.a.johansson@slu.se.




SLU
SCIENCE AND EDUCATION FOR SUSTAINABLE LIFE