Gäller för: Västra Götalandsregionen
Innehållsansvar: Fredrika Holm Fredriksson, (freho10), Strateg
Granskad av: Fredrika Holm Fredriksson, (freho10), Strateg
Godkänd av: Johan Flarup, (johfl), Direktör

Giltig från: 2025-03-18
Giltig till: 2027-03-18

Hantering av sårbarheter i IT-miljö

Regional rutin 2025–2029

Ledningssystem för informationssäkerhet och dataskydd

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

1 Inledning

Mål: Information om tekniska sårbarheter i informationsbehandlingsresurser som används ska inhämtas och organisationens exponering för sådana sårbarheter granskas och lämpliga åtgärder vidtas.

Sårbarhetshantering är en viktig aktivitet i det systematiska informationssäkerhetsarbetet i syfte att bibehålla informationssäkerheten. Med sårbarhet menas "brist i skyddet av en tillgång eller av en säkerhetsåtgärd som kan utnyttjas av ett eller flera hot"[1].

Hantering av sårbarheter i IT-miljö innebär att tekniska sårbarheter identifieras och riskerna med dessa sårbarheter utvärderas. Bedömning görs huruvida sårbarheterna kan korrigeras och risken minimeras eller sårbarheten och medföljande risk kan accepteras, till exempel om effekterna av en utnyttjad sårbarhet är försumbara eller betydligt mindre än kostnaden för att åtgärda sårbarheten.

Regional rutin för hantering av sårbarheter i IT-miljö är styrande för alla förvaltningar och bolag i Västra Götalandsregionen (VGR) och ingår som en del i ledningssystemet för informationssäkerhet och dataskydd (LISD). Rutinen fastställer den styrning av sårbarhetshantering som ska användas i VGR. Hantering av sårbarheter detaljeras i en kompletterande tillämpningsanvisning.

Rutinen utgår från Informationssäkerhet och dataskydd – Regional riktlinje 2023-2027 (RS 2023-02811) och avser implementation av säkerhetsåtgärder enligt ISO 27002:2022 avsnitt 8.8 ”Hantering av tekniska sårbarheter” samt tillägg för dataskydd enligt ISO 27701:2021.

2 Termer och begrepp

IS/IT-tjänst	Kan vara enskild applikation, tjänst eller plattform eller större system och plattformar.
Sårbarhet	brist i skyddet av en tillgång eller av en säkerhetsåtgärd som kan utnyttjas av ett eller flera hot

[1] MSB: Termbanken för informationssäkerhet - https://termbank-informationssakerhet.msb.se/

Sårbarhetshantering	Processen för att identifiera, utvärdera, hantera, minska och åtgärda sårbarheter i organisationens IT-miljö
Sårbarhetsskanning	Genomförs med hjälp av specifik mjukvara för att identifiera sårbarheter i nätverk, datorinfrastruktur och plattformar eller applikationer
Teknisk sårbarhet	Sårbarhet i den tekniska lösning som direkt bygger upp IS/IT-tjänst. Till exempel konfiguration, tillåtna protokoll, ej supporterade versioner av mjukvara, lösning för identitet och åtkomst, osv. Sårbarhet i fysisk kringliggande infrastruktur så som dörrar eller brandskydd hör inte till denna rutin.
Tillämpningsanvisning	Anvisning för tillämpning av säkerhetsåtgärder enligt LISD och ISO 27002.
Ägare IS/IT-tjänst	En ägare av IS/IT-tjänst ansvarar för tillämpning av säkerhetsåtgärder för tjänsten. Ägare IS/IT-tjänst kan utgöras exempelvis av någon av produktområdesansvarig, produktansvarig, tjänsteägare, tjänsteområdesansvarig, systemägare eller applikationsägare för enskild applikation, tjänst, plattform eller större system och plattformar.

3 Ansvar och roller

3.1 Informationsägare

Informationsägare ansvarar övergripande för riskhantering av informationstillgång. Enskilda risker kan tilldelas en riskägare som ansvarar för dess hantering.

3.2 Regional processägare

När informationstillgångarna ingår i regiongemensamma processer, regiongemensamma IS/IT- tjänster, projekt och/eller upphandlingar företräds flera myndigheters informationsägare av en regional processägare.

3.3 Informationssäkerhetschef

Informationssäkerhetschef ansvarar för VGR:s regionala process för sårbarhetshantering, inklusive kompletterande tillämpningsanvisning för sårbarhetshantering.

Informationssäkerhetschef ansvarar för att följa upp sårbarhetshanteringen som ett led i uppföljning av ledningssystemet för informationssäkerhet och dataskydd.

Informationssäkerhetschefen ansvarar också för att, som en del av sårbarhetshanteringsprocessen, identifiera sårbarheter genom scanning.

3.4 Digitaliseringsdirektör

Digitaliseringsdirektör ansvarar för utförandet av sårbarhetshantering i VGR:s IT-miljö.

3.5 Ägare IS/IT-tjänst

Ägare IS/IT-tjänst ansvarar för hantering och rapportering av sårbarheter kopplat till den produkt eller tjänst denne är ansvarig för, exempelvis printertjänst (produktansvarig print), regionala applikationer (respektive applikationsägare/ansvarig), förvaltningsspecifika applikationer. För nätverk, plattformar och applikationer som driftas av extern leverantör ska leverantören upptäcka, rapportera och hantera kritiska sårbarheter utan dröjsmål och övriga sårbarheter enligt avtal. Leverantör utför detta självständigt eller med stöd av ägare IS/IT-tjänst i VGR.

4 Sårbarhetshantering

En sårbarhet är en brist i skyddet av en tillgång eller av en säkerhetsåtgärd som kan utnyttjas av ett hot eller flera hot.

Förekomsten av cyberbrott, och de risker detta för med sig, tvingar VGR att fokusera mer på informationssäkerhet. Många av de intrång som sker i organisationers IT-miljöer sker genom att en angripare utnyttjar en sårbarhet som inte har upptäckts eller hanterats i tid.

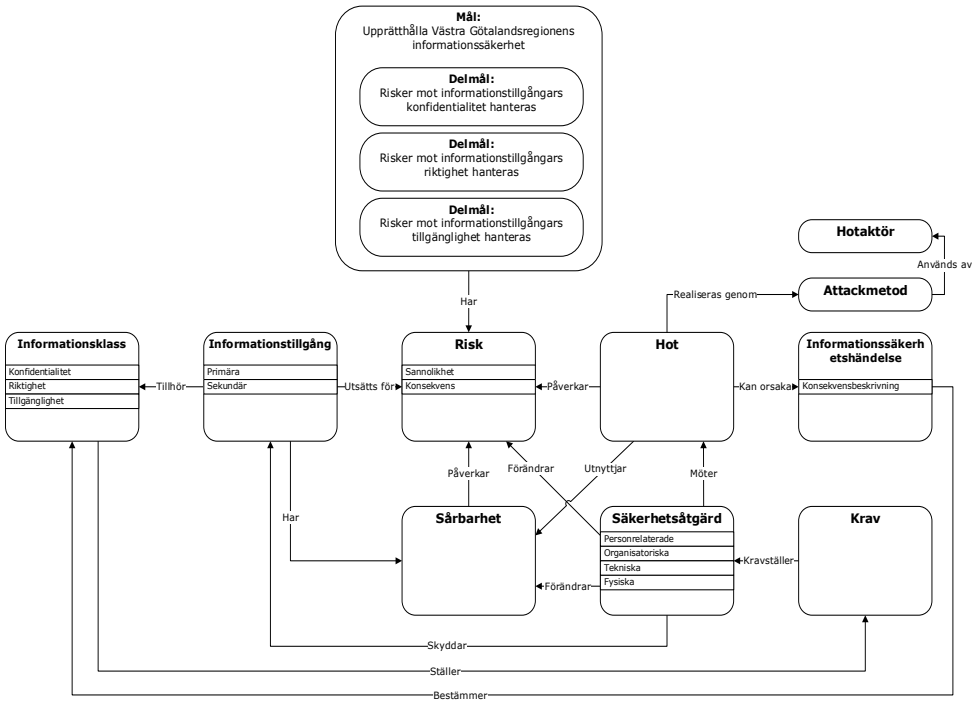
En sårbarhetshanteringsprocess är en del av en VGR:s strävan att kontrollera informationssäkerhetsrisker. Sårbarhetshantering gör det möjligt för VGR att få en kontinuerlig översikt över sårbarheter i IT-miljön och de risker som är förknippade med

dem. Genom att identifiera och hantera sårbarheter i IT-miljön kan VGR försvåra för angripare att tillskansa sig eller skada informationstillgångar.

Sårbarhetshantering i IT-miljö innebär att sårbarheter identifieras och riskerna med dessa sårbarheter utvärderas, bedöms och hanteras utifrån den risk sårbarheten innebär. Exempelvis kan avhjälpande åtgärd anstå om effekterna av en attack kan konstateras vara låga eller om kostnaden för korrigering är högre än eventuella skador för verksamheten i bred bemärkelse.

Hantering av sårbarheter i IT-miljö omfattar i första hand sårbarheter i tekniska informationsbehandlingsresurser. Eftersom dessa används för informationsbehandling är kopplingen tydlig även till informationstillgång och risker och hot mot denna. Informationsägare ska därför hållas informerad om ej åtgärdade sårbarheter och resultat av säkerhetsåtgärder för att kunna hålla riskanalys för informationstillgång uppdaterad.

Tillämpliga regelverk ska följas vid arbetet. Exempelvis behöver det bedömas om sårbarheten kan orsaka en allvarlig driftstörning enligt kriterier för NIS-incidenter vilka ska rapporteras enligt VGR:s regionala rutin för incidenthantering. Sårbarheter i system som utgör eller innehåller medicintekniska produkter eller nationella medicinska informationssystem ska värderas för anmälan till tillverkaren och Läkemedelsverket som en brist i produkten.



Figur 1 - Element i riskhanteringsprocessen. Ur Regional rutin riskhantering för informationssäkerhet

5 Process sårbarhetshantering

En teknisk sårbarhet kan upptäckas på flera olika sätt. Det kan exempelvis vara genom schemalagd skanning för upptäckt av kända sårbarheter, vid genomförande av penetrationstester, riskanalys, vid omvärldsbevakning, hotunderrättelser, belastningstester eller vid utredning av ett säkerhetsangrepp.

Huvudsyftet med sårbarhetshanteringsprocessen är att upptäcka och åtgärda sårbarheter i rätt tid. Sårbarhetsskanningar och omvärldsbevakningar ska därför genomföras regelbundet för att hitta och kunna agera på sårbarheter snabbt efter att de uppstått. Årliga skanningar innebär hög risk eftersom tiden till upptäckt av sårbarhet kan bli lång. VGR ska i normalfallet skanna IT-miljö, system och tjänster minst 1 gång/månad.

Sårbarhetshantering för eventuell IS/IT-tjänst som inte hanteras regionalt ska också följa styrningen i denna rutin. Eftersom VGR till stor del har en IT-miljö där de flesta datorer, servrar, applikationer och andra delar kan nå de flesta andra datorer, servrar, applikationer och andra delar så behöver även den svagaste länken vara stark för att reducera risken för spridningseffekter av lyckade angrepp mot någon IS/IT-tjänst.

Sårbarhetshanteringsprocessen behöver minst bestå av följande:

1. Kartläggning av alla IS/IT-tjänster som ska sårbarhetshanteras
2. Systematiskt arbete för att upptäcka sårbarheter. Exempel:
    a. Omvärldsbevakning globalt och i närområdet
    b. Insamling och analys av hotunderrättelser
    c. Varningar
    d. Händelser som rapporterats av personal
    e. Regelbunden sårbarhetsskanning. Även externa tjänster ska skannas av VGR och/eller leverantör.
3. Bedömning av sårbarheten, bedömning av vilka risker som sårbarheten medför samt rapportering av sårbarheter till informationsägare och informationssäkerhetsfunktionen
4. Genomföra avhjälpande åtgärder
5. Följa upp vidtagna åtgärder

6 Värdering av sårbarhet

Oavsett om en sårbarhet identifieras vid skanning, penetrationstest, genom manuell undersökning, tips, riskanalys, eller vid utredning av ett säkerhetsangrepp så ska sårbarheter bedömas och prioriteras för åtgärd.

Tillämpningsanvisning för hantering av sårbarheter i IT-miljö styr sårbarhetsvärdering av IS/IT-tjänster i VGR. Grunden för sårbarhetsvärderingen är Common Vulnerability Scoring System (CVSS), men den kompletteras med fler faktorer för att utgöra en mer komplett så kallad Risk-Based Vulnerability Management (RBVM).

För sårbarhetsvärderingar som inte kan genomföras med RBVM används enbart Common Vulnerability Scoring System (CVSS), som är en öppen och gratis internationell standard med en värderingsskala för sårbarheter. Både tillverkare och leverantörer av IT tjänster använder CVSS. Varje identifierad sårbarhet tilldelas ett värde mellan 0–10. Risk ska bedömas utifrån detta CVSS värde enligt nedan:

Allvarlighet	CVSS v3	Definition
CVSS 9,0-10,0 Kritisk	9,0-10,0	Det är relativt okomplicerat att utnyttja sårbarheten och detta resulterar vanligtvis i att systemet kompromitteras. Det rekommenderas att göra en handlingsplan och patcha omedelbart.
CVSS 7,0-8,9 Hög	7,0-8,9	Utnyttjande är svårare men kan orsaka förhöjda privilegier och potentiellt förlust av data eller stillestånd. Det rekommenderas att utforma en handlingsplan och patcha så snart som möjligt.
CVSS 4,0-6,9 Måttlig	4,0-6,9	Sårbarheter finns men kan inte utnyttjas eller kräver extra steg som social ingenjörskonst. Det rekommenderas att skapa en handlingsplan och patcha efter att högprioriterade problem har lösts.
CVSS 0,1-3,9 Låg	0,1-3,9	Sårbarheter finns men är icke-exploaterbara i dagsläget. Att åtgärda sårbarheten minskar en organisations attackyta. Det rekommenderas att skapa en handlingsplan och patcha under nästa underhållsfönster.
CVSS N/A Ingen	N/A	Det finns ingen sårbarhet. Ytterligare information tillhandahålls om föremål som uppmärksammats under testning, starka kontroller och ytterligare dokumentation.

Figur 2 – CVSS översikt nivåer och allvarlighet

Kritiska sårbarheter i VGR:s externa samt interna tjänster ska åtgärdas utan dröjsmål. Höga sårbarheter ska åtgärdas så snart som möjligt, dvs vid nästa möjliga tillfälle när det kan göras utan att påverka leverans av tjänsten negativt. Åtgärder för sårbarheter

med låg och måttlig risk planeras in och prioriteras under normal förvaltning av påverkad IS/IT-tjänst.

Om åtgärd saknas eller inte kan genomföras för kritisk eller hög sårbarhet, ska nedstängning eller isolering av tjänsten övervägas till dess åtgärd finns på plats alternativt kortare tidsfrist för åtgärd beslutas.

7 Relaterade dokument

Riktlinje för informationssäkerhet och dataskydd (RS 2023-02811)

Regional rutin riskhantering för informationssäkerhet (2024-2028)

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Fredrika Holm Fredriksson, (freho10), Strateg

Granskad av: Fredrika Holm Fredriksson, (freho10), Strateg

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-332

Version: 2.0

Giltig från: 2025-03-18

Giltig till: 2027-03-18