Dnr UFV 2014/1307

UPPSALA
UNIVERSITET

Riktlinjer för informationssäkerhet

Säker systemutveckling

Fastställda av Säkerhetschef 2014-10-28

Innehållsförteckning

1 Inledning

Dagens internetbaserade IT-miljöer, ständigt utsatta för nya hot relaterade till säkerhet, ställer särskilda krav i allt arbete som bedrivs med utveckling och underhåll av IT-baserade system. Att använda utvecklingsmetoder och rutiner som inkluderar moment där särskilt fokus ligger på säkerhetsmässiga aspekter utgör en grundläggande förutsättning för säker drift av de system som utvecklas.

I de riktlinjer för informationssäkerhet som fastställts av universitetsdirektören, Dnr UFV 2010/424, uttrycks följande med särskild koppling till projekt- och förvaltningsarbete som inbegriper systemutveckling:

- En risk- och hotbildsanalys enligt anvisningarna för risk- och hotbildsanalyser ska genomföras i alla utvecklings- och anskaffningsprojekt. Ansvarig för att så sker är projektägare/motsvarande.

- Planering och uppföljning av skyddsåtgärder ska göras som en del av det löpande förvaltningsarbetet med befintliga informationssystem. Ansvarig för att så sker är Systemägare/motsvarig.

Detta dokument avser att, tillsammans med ovanstående punkter, beskriva universitetets riktlinjer för säker systemutveckling.

2 Ansvar

2.1 Efterlevnad

Ansvaret för efterlevnad av dessa riktlinjer fördelar sig enligt följande:

Projektägare/motsvarande har det övergripande ansvaret i samband med systemutvecklingsprojekt.

Systemägare, objektägare/motsvarande har det övergripande ansvaret i det löpande förvaltningsarbetet.

Projektledare, förvaltningsledare/motsvarande ansvarar för att riktlinjerna beaktas i det dagliga arbetet med systemutveckling samt att eventuella konsulter har kännedom om dessa.

Systemutvecklare ansvarar för att riktlinjer med direkt påverkan på utvecklingsarbetet följs.

2.2 Uppdatering av riktlinjerna

Säkerhetschefen ansvarar för att riktlinjerna kontinuerligt uppdateras och att underliggande stöddokument fastställs.

3 Definitioner

Informationsklassificering utgör ett moment där information som hanteras, exempelvis av IT-system, bedöms utifrån aspekterna konfidentialitet (sekretess), riktighet och tillgänglighet. Informationens behov av säkerhetsmässiga åtgärder bestäms i en behovsskala bestående av nivåerna basnivå, hög nivå samt särskilda krav.

SQL injection är ett sätt att utnyttja säkerhetsproblem i hanteringen av indata i system som arbetar mot en databas. Injektionen sker genom att en användare skickar in parametrar till en databasfråga, utan att parametrarna transformeras korrekt med avseende på speciella tecken. Med anpassade parametrar kan en användare kringgå inloggningssystem och manipulera data.

Cross Site Scripting, XSS, används som metod för att stjäla information eller förstöra en webbsidas utseende. Metoden är tillsammans med SQL injection omnämnd som en av de mest kritiska säkerhetsriskerna med koppling till webbapplikationer (se information från den globala organisationen Open Web Application Security Project (OWASP), https://www.owasp.org)

2-faktor autentisering är en metod för inloggning där den inloggade identifierar sig med något som personen ifråga känner till, exempelvis ett lösenord, samt därtill med något som personen har i sin ägo, exempelvis en s.k. Yubikey som placeras i en av datorns USB-portar.

4 Omfattning

4.1 Övergripande

Universitetets IT-system ska vara utformade i enlighet med kraven i offentlighetslagstiftningen och andra tillämpliga lagar och regler. Om osäkerhet råder ska universitetets juridiska avdelning tillfrågas.

4.2 Identifiering av säkerhetskrav före utveckling

- Säkerhetskrav ska identifieras och dokumenteras i ett utvecklingsprojekts inledande fas. Systemägare, projektledning och projektdeltagare i olika roller ska tillsammans överenskomma vilka säkerhetskrav som ska gälla. Universitetets säkerhetsenhet bidrar med råd och stöd.
- Information som hanteras i systemet ska klassificeras med avseende på skyddsbehov. Uppgifter som markering för skyddad identitet och lösenord utgör exempel på uppgifter med högt ställda krav på sekretess.
- En riskanalys ska genomföras i alla utvecklings-, vidareutvecklings- och anskaffningsprojekt.

Anvisningar och blanketter för genomförande av informationsklassificering och risk- och hotbildsanalyser finns i Medarbetarportalen under STÖD OCH SERVICE, Säkerhet.

4.3 Angående källkod

- Åtkomst till källprogramkoden ska kontrolleras av ett behörighetssystem.
- All källkod ska versionshanteras. Alla förändringar som görs i koden ska loggas.

4.4 Bearbetning, indata och utdata

Metoder för att säkerställa korrekt bearbetning ska användas. Dessa metoder bör innefatta moment som kodgranskning, rutiner för validering av indata samt rimlighetskontroller av utdata. Det finns anledning att vara särskilt uppmärksam på brister i programkoden som gör denna känslig för fenomen som SQL injection och Cross Site Scripting (XSS), då dessa utgör exempel på särskilt vanligt förekommande sårbarheter.

4.5 Säker kommunikation/säker lagring av information

- Dataöverföringar av känsliga data ska alltid ske via krypterad transport, https-anslutning eller motsvarande.

- Krypterad lagring av känslig information ska övervägas för information som vid informationsklassificering klassats till *hög nivå*.
- Vid överföring av känslig information till annat system ska motsvarande skyddsåtgärder som vidtas inom det egna systemet vara vidtagna i kommunikationen samt i det mottagande systemet.

4.6 Autentisering/åtkomst till databaser, filer och källkod

- Universitetets standardiserade användaridentiteter och autentiseringssystem ska användas så långt det är möjligt.
- Moment som autentisering och auktorisering ska vara väldefinierade i systemets tjänsteskikt.
- Systemanvändare ska ha en unik användaridentitet, dvs. inga gruppidentiteter får finnas.
- Lösenord ska följa universitetets riktlinjer för lösenordshantering.
- Om särskilt känslig information hanteras av systemet ska s.k. tvåfaktorautentisering övervägas.
- Åtkomst till databaser, filer och källkod till programmen ska styras på ett säkert sätt. Dokumenterade rutiner för behörighetstilldelning ska finnas och följas.
- Det ska gå att begränsa användares åtkomst till system och databaser utifrån parametrar som roll, organisationstillhörighet och liknande.

4.7 Loggning

- Systemet ska inkludera rutiner som skapar erforderliga loggar för uppföljning av säkerheten i systemet. Operatörers inloggningar och andra viktiga säkerhetsrelaterade händelser i systemet ska alltid loggas.
- Säkerhetsloggar ska skyddas mot obehörig åtkomst och oavsiktlig förändring samt sparas på ett säkert sätt.
- Säkerhetsloggar ska skickas krypterat till syslog-server enligt instruktioner som återfinns i Medarbetarportalen under STÖD OCH SERVICE, Säkerhet, Riktlinjer och stöddokument.
- Tidsrymd för sparande av transaktionsloggar ska avtalas med driftsleverantören.

4.8 Test och testdata

- Utvecklings- och testarbete ska utföras i en egen, från driften väl avskild, miljö.
- I ett fall då data i en testmiljö är baserad på verklig data, ska testmiljön omgärdas av säkerhetsåtgärder motsvarande de som används i produktionsmiljön.
- Rutiner ska finnas för att säkerställa att testdata kontrolleras och skyddas.

4.9 Överlämnande till drift/fortsatt förvaltning av systemet

- Vid driftsättning ska systemet överlämnas till systemförvaltning enligt en dokumenterad rutin för detta. En fastställd organisation för systemförvaltning ska finnas och vara känd av både överlämnande och mottagande parter.
- Dokumentation som beskriver systemet och dess kopplingar till andra system ska finnas framtagen innan systemet överlämnas för drift och fortsatt förvaltning.
- Rutiner för godkännande av systemförändringar ska finnas och följas.
- Alla föreslagna systemändringar ska granskas för att säkerställa att de inte äventyrar säkerheten vare sig i systemet eller i driftmiljön.