RIKSGÄLDEN
SWEDISH NATIONAL DEBT OFFICE

Krav på leverantörer och på dess produkter avsedda att användas för myndigheters betalningar över Internet

1 Krav på leverantörens organisation

1.1 Informationssäkerhetsmässiga krav

Leverantören ska följa de relevanta säkerhetsrekommendationer som är utfärdade av:

- MSB - Myndigheten för samhällsskydd och beredskap
- Tekniska Specifikationer enligt SIS standard
- Statskontoret (Nyttjande av IT inom offentlig förvaltning)
- Riksgäldskontoret (Betalningar)

Notera även att särskilt följande lagar bör beaktas:

- PUL - Personuppgiftslagen
- Bokföringslagen
- Lagstiftning om överföring av kapital över n ationsgränser

1.1.1 ISO 27000-serien

Leverantören ska ha ett internt säkerhetsarbete lägst i nivå med svensk standard ”Ledningssystem för informationssäkerhet” (LIS) och ”Riktlinjer för styrning av informationssäkerhet” enligt SS-ISO/IEC 27001/27002.

Detta krav innebär inget krav på certifiering men däremot att man för det interna säkerhetsarbetet hanterar samtliga delar i standarden på ett sätt som motsvarar standardens krav på ett genomtänkt och gott informationssäkerhetsarbete.

Standarden består av följande delar, följt av en kort beskrivning av vad varje del representerar:

- **Informationssäkerhetspolicy**
  - Framtagning och underhåll av en informationssäkerhetspolicy.
- **Organisation av informationssäkerhet**
  - Engagemang från ledningen att integrera informationssäkerhet ut i organisationen. Roller och ansvar ska definieras, avtal med externa leverantörer och övriga externa parter ska regleras så att säkerheten bibehålls.
- **Hantering av tillgångar**
  - Identifiering av leverantörens tillgångar och vem som äger dem.
  - Klassificering av information.
- **Personal och säkerheten**
  - Fastställda rutiner före, under och efter anställning av personal.
  - Dokumentation av roller och ansvar i enlighet med policy.
  - Utbildning av personal för ökad informationssäkerhetsmedvetenhet.
- **Styrning av kommunikation och drift**
  - Framtagning av driftsdokumentation.
  - Rutiner för skydd mot skadlig kod.
  - Rutiner för säkerhetskopiering.
  - Säkerhet i nätverk.
  - Rutiner för hantering av media.
  - Övervakning och loggning av nätverk.
- **Styrning av åtkomst**
  - Användarbehörighet och kontroll av åtkomst till informationssystem.
  - Styrning av användaråtkomst till nätverk och operativsystem.
  - Rutiner för distansarbete.
- **Anskaffning, utveckling och underhåll av informationssystem**
  - Säkerhet ska integreras i alla delar av leverantörens informationssystem. Detta innefattar tekniska aspekter såsom validering av in- och utdata, kryptering och nyckelhantering samt säkerhet i databaser och filer.

- **Hantering av informationssäkerhetsincidenter**
  - Rutiner för rapportering av incidenter och hur dessa åtgärdas.

- **Kontinuitetsplanering**
  - Om avbrott sker i verksamheten ska det finnas plan på återställning.

- **Efterlevnad**
  - Säkerställ att leverantören följer rättsliga krav (lagar, mm), policys och standarder, samt att revisioner görs kontinuerligt.

1.1.2 Relevanta delar av "Ramavtal för bankerna"
Leverantören skall följa de delar av "Ramavtal för bankerna" som är relevanta för leverantören, dess organisation och produkt. Exempel på krav som skulle kunna vara relevanta är:
- Behörighetsadministration
- Uppföljning av teknisk säkerhet
- Övervakning och logganalys
- Autentisering
- Krav på användargränssnitt
- Sessionshantering
- Krav på lösenord
- Krav på förbindelser
- Krav på kryptografisk teknik

1.2 IT-miljö
Leverantören förväntas följa följande krav som är baserade på best practices inom ITsäkerhetsbranchen. För varje punkt gäller att undantag skall vara baserade på ett affärsbehov samt vara dokumenterade. Denna dokumentation skall innehålla skälet till undantaget.

a) Leverantören ska ha en brandvägg, denna skall vara konfigurerad att som standard neka trafik. All trafik som tillåts passera brandväggen skall vara baserad på affärsbehov samt vara dokumenterad, inklusive skälet till att trafiken måste tillåtas.
b) Nätverket skall vara segmenterat så långt som möjligt, detta innebär i praktiken att alla enheter på nätverket skall sitta på egna subnät.
c) Grundregeln för enheter anslutna till nätverket skall vara "en enhet – en funktion".
d) Leverantören skall ha system för att upptäcka intrång i sin IT-miljö och detta system skall förväntas upptäcka pågående intrång.
e) Leverantören skall ha konfigurerat nätverksanslutna enheter på sådant sätt att forensiska utredningar i efterhand är genomförbara. Detta inkluderar bland annat:
   - Lyckade och misslyckade in- och utloggningar.
   - Lyckade och misslyckade filöppningar från gemensamma utrymmen såsom utdelade nätverksenheter.
   - Icke normal nätverkstrafik t.ex. filöverföringar efter kontorstid.
   - All metadata om Internettrafik.

2 Krav på Leverantörens produkt
2.1 Relevanta delar av "Ramavtal för bankerna"
Leverantörens produkt förväntas uppfylla relevanta krav ur "Ramavtal för bankerna". Se punkt 1.1.2.

2.2 IT-säkerhetsmässiga krav på produkten
2.2.1 OWASP Top 10
Webb-baserade produkter skall ha skydd så att det inte går att göra lyckade angrepp mot produkten med någon av de attackmetoder som finns beskrivna i OWASP Top 10-listan[1].

2.2.2 Webb-baserade produkter
Webb-baserade produkter skall utvecklas:

a) så de använder HTTPS/TLS som standard.
b) så de fungerar bakom en reverse-proxy.
c) så de fungerar bakom en applikations-brandvägg.
d) så de fungerar bakom en SSL-accelerator.
e) så de fungerar bakom en lastbalanserare eller motsvarande lösning.
f) utan användning av ActiveX.
g) så systemet inte är begränsat till ett specifikt webbläsarfabrikat eller en specifik webbläsarversion.

2.2.3 CERT Top 10 Secure Coding Practices
De utvecklare som utvecklar produkten skall ha läst och förstått CERT Top 10 Secure Coding Practices och Bonus Secure Coding Practices[2] samt arbeta enligt dessa.

2.2.4 Validering av indata

a) Indata skall kontrolleras mot vitlistor så att dess värden är acceptabla.

[1] *http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project*
[2] *https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices*

b) Även data som anses komma från betrodda källor är indata och skall kontrolleras enligt punkten ovan. Till exempel data som hämtas från en databas eller läses från disk.
c) Hur produkten hanterar indata, vare sig indatat är inom giltiga värden eller ej, skall vara deterministiskt.

2.2.5 Produktdesign

a) All kommunikation till och från komponenter skall krypteras.
b) Leverantören skall tillhandahålla godkända krypteringsmekanismer och funktioner för säker åtkomst till produkten.
c) En produkt som använder sig av en databas skall vara designad så att databasen inte behöver installeras på samma server eller nätverk som applikationsservern.
d) Personliga konton skall användas vid åtkomst mot databas, applikationskonton får ej användas.
e) Produkten får inte vara designad så att den kräver administrativa privilegier för att fungera. (root, Local Admin eller liknande).
f) Produkten får inte kräva att användaren har administrativa privilegier. (root, Local Admin eller liknande).
g) Förutsättningar om miljön produkten används i skall undvikas så långt det är möjligt.
h) Om ett standard operativsystem används får produkten inte ha sådana förutsättningar på sin miljö att operativsystemet inte kan härdas.
i) All säkerhetsrelevant konfiguration av produkten skall hanteras via gränssnitt eller API.
j) Säkerhetsuppdateringar av samtliga komponenter (exempelvis applikationsserver, databas och operativsystem) ska kunna genomföras utan att produktens funktionalitet förändras. Produkten får aldrig ställa krav på att underliggande komponenter inte säkerhetsuppgraderas (patchas) eller uppdateras.
k) Leverantören skall dokumentera hur uppgraderingar av underliggande komponenter skall genomföras samt hur tester bör genomföras för att minimera kompabilitetsproblem.
l) Produkten skall använda autentisering vid kommunikation mellan aktuella system.
m) I en klient-server-miljö skall identifiering, behörighetskontroll och loggning ske på servern.
n) Produkten skall behålla säkerhetsinställningar även efter omstart.
o) Produkten får aldrig kräva eller förlita sig på osäkra tjänster och protokoll, t.ex. NFS, telnet, rlogin, FTP eller NetBIOS.
p) Endast filsystem som har stöd för behörighetskontroll med access-listor eller motsvarande skall användas.

2.2.6 Kvalitetssäkring

a) Samtliga utvecklare och projektledare som arbetar med produkten skall ha läst och förstått ”The Joel Test: 12 Steps to Better Code”[3].
b) Samtliga utvecklare av produkten skall minst känna till de av följande begrepp inom säker programmering som är relevanta för produkten samt hur man programmerar för att vara skyddad mot de sårbarheter dessa begrepp behandlar:
    - Buffer overflow
    - One byte overflow
    - Integer wrap
    - Heap overflow
    - Double free
    - Race condition
        - Signal race
        - Tmp race
    - Injektionsbaserade attacker
        - SQL-injektion
        - Kod-injektion
            - XSS/Javascript-injektion
            - PHP/ASP/Perl/VB/Awk-injektion
        - Kommando-injektion
        - Null-byte-injektion
        - CR/LF-injektion
    - IFS-stils-attacker
c) Leverantören skall ha en kvalitetssäkringsprocess för produkten.
d) Alla delar av produkten skall vara av produktionskvalitet.
e) Alla delar av produkten skall vara kvalitetstestade.

2.2.7 Kodgranskning

Kodgranskning skall utföras av oberoende part, minst vid varje huvudrelease av produkten. Eventuella brister som upptäckts skall vara åtgärdade innan produkten tas i drift.

[3] *http://www.joelonsoftware.com/articles/fog0000000043.html*

2.2.8 Leverans

Vid leverans av produkten gäller att:

a) produkten inte får innehålla standard-lösenord.
b) produkten inte får innehålla testdata eller liknande.
c) alla eventuella bakdörrar, ”emergency codes”, procedurer för återställning av

lösenord och liknande skall vara dokumenterade.

d) dokumentation av hur minsta möjliga öppning i en brandvägg ser ut för att produkten skall fungera skall medfölja.
e) intyg skall uppvisas på att produkten är säkerhetstestad, hur den är säkerhetstestad, vad som är säkerhetstestat samt att produkten har klarat testerna med godkänt resultat.

Besöksadress: Jakobsbergsgatan 13 • Postadress: SE-103 74 Stockholm • Telefon: 08 613 45 00 • Fax: 08 21 21 63
E-post: riksgalden@riksgalden.se • Webbadress: www.riksgalden.se