Mars 2022
Bilaga 3

Säkerhetsbilaga IA-systemet

Innehållsförteckning

1 Inledning

Afa Trygg tjänstepensionsaktiebolag org. nr. 516401-8615 (Leverantören) strävar efter att upprätthålla en god säkerhet för såväl intern information som våra kunders information. För att göra det genomförs ett strukturerat arbete vars resultat utvärderas regelbundet med syfte att ständigt förbättra säkerheten för informationen.

Denna säkerhetsbilaga redovisar för hur Leverantören arbetar för att uppnå god säkerhet för sina kunders information som hanteras i systemet ”Informationssystem för Arbetsmiljö”, härefter kallat för IA-systemet.

Bilagan inkluderar även ett kapitel som avser krav som Leverantören ställer på sina användarföretag, samt vilka möjligheter och skyldigheter användarföretagen har att bidra till säkerhetsarbetet.

Frågor gällande Leverantörens arbete för god informationssäkerhet kan ställas till Leverantörens Säkerhetschef via IA support.

2 Styrande dokument

Via internt styrande dokument, exempelvis för systemutveckling, incidenthantering säkerställer Leverantören att den operationella säkerheten upprätthålls vid drift och förvaltning av IA-systemet.

3 Organisation

Säkerhetsfunktion

En säkerhetsfunktion finns uppsatt som internt arbetar integrerat med verksamheten och bistår linjeorganisationen med kompetens, utvärderingar, och riktlinjer för informations- och IT-säkerhet. Säkerhetsfunktionen hanterar frågor gällande såväl IT-säkerhet som fysisk säkerhet och personalsäkerhet.

CERT (Computer Emergency Response Team)

För hantering av cyberattacker sätts ett team samman med kompetenser inom bl.a. kommunikationssäkerhet, klientskydd, Datacenter, Microsofts samt Unix infrastruktur. Vid behov kan även andra kompetenser allokeras.

4 Personalsäkerhet

Samtlig personal, såväl egen som inhyrd, skriver på avtal om tystnadsplikt innan åtkomst till IT-system. Personal som arbetar med IA-systemet får utbildning om hur IA-systemet nyttjas och vilka restriktioner som finns. Regelbundna samtal med egen personal nyttjas för att upptäcka och förebygga otillbörligt agerande.

5 Hantering av tillgångar

Med hänsyn till att personuppgiftsrelaterad information hanteras i IA-systemet, klassificeras denna som konfidentiell. Detta innebär att Leverantören arbetar aktivt med behovsstyrd behörighetstilldelning via roller. Endast behörigheter nödvändiga för att utföra sina arbetsuppgifter tilldelas personalen.

6 Styrning av åtkomst

6.1 Inom Leverantören

Endast ett fåtal personer inom Leverantörens driftsavdelning har fulla rättigheter till databaser och diskar. Teamet från Leverantörens systemutvecklingsavdelning som arbetar med utveckling av IA-systemet har läsrättigheter i databasen, men inga rättigheter till diskar. Alla inloggningar i IA-systemet görs via personliga konton och loggas i den centrala logghanteringen.

Leverantörens supportpersonal för IA-systemet kan för att ge korrekta svar gällande inkomna supportfrågor, behöva koppla upp sig mot användarföretaget och därigenom ta del av användarföretagets data. Detta görs enbart efter skriftligt godkännande från användarföretaget. Alla läsningar av data i IA-systemet loggas för varje enskilt ärende. Dessa loggar finns tillgängliga i IA-systemet för behörig personal hos användarföretaget.

6.2 För användarföretag

Leverantören upprättar och tilldelar endast behörigheter för administratörer hos användarföretagen. Användarföretagen är därefter själva ansvariga för att administrera användare av IA-systemet inom sin organisation. Behörigheter styrs via roller, vilka tilldelas användare via administratörerna. Användarföretagens användare, administratörer såväl som övriga användare, har möjlighet att ange en tidsbegränsad ersättare för sin behörighet.

Användarföretag ansvarar själv för inloggningsmetod, t ex. via användarnamn/lösenord, SSO via SAML 2.0, eller en kombination av dessa. Leverantören rekommenderar SSO via SAML 2.0

7 Kryptering

Kommunikation sker krypterat via HTTPS (TLS 1.2 eller högre). Dokumenterade rutiner för hantering och uppdatering av kryptografiskt material såsom nycklar för certifikat är etablerade.

Databas och diskar är krypterad.

8 Fysisk och miljörelaterad säkerhet

Den fysiska säkerheten i våra datorhallar består av inbrottslarm, brandskydd, inpasseringssystem samt kameraövervakning.

Inbrottslarmet är kopplat till ett bevakningsföretag med kort inställelsetid. Driftsmiljön patrulleras av väktare, detta sker med oregelbundna intervall och minst två gånger per dygn.

Brandskyddet består av såväl rökdetektorer vilka är kopplade till räddningstjänsten som automatisk släckutrustning.

System för skydd mot strömavbrott finns.

Endast behörig personal har fysisk åtkomst till datorhallarna, access till datorhallarna är behörighetsstyrd. Inpasseringssystemet loggar såväl lyckade som misslyckade försök till fysisk åtkomst.

9 Utrustning

Data på digitala medier som utrangeras raderas, därefter destrueras de digitala medierna. Detta sker på en sekretessanläggning av säkerhetsgodkänd personal.

10 Driftssäkerhet

10.1 Kommunikation

Datorhallarna som nyttjas är anslutna till Internet via två separata leverantörer. En funktion för automatisk failover mellan leverantörerna nyttjas för att säkerställa hög tillgänglighet.

IA-systemet är avgränsat från övriga IT-system inom Leverantören via brandväggar. Endast kommunikation som explicits har tillåtits kan passera brandväggarna.

Avseende sabotageförsök genom så kallade ’denial of service’ skyddar Leverantören sin miljö genom inbyggd teknologi i brandvägg samt genom internetoperatörens försorg. Stora belastningsattacker väntas ut. Begränsad eller otillgänglig service vid sådant tillfälle är en accepterad risk.

10.2 Spårbarhet och övervakning

Central logghantering nyttjas för IA-systemet samt för relaterad nätverkskommunikation. Utsedd personal arbetar aktivt med att upptäcka riskfyllda händelser via regelbaserade alarm samt verktyg för avvikelseanalys. Vid behov kan relevanta delar av loggarna göras tillgänglig för kundföretag.

Data skyddas via behörigheter som kontrolleras på alla nivåer i IA-systemet. Hantering av data loggas, såväl läsning, editering samt

inloggning. Även misslyckade inloggningsförsök loggas.

IA-systemets tid hämtas från systemets servrar. Loggade tider presenteras i användarbrowserns tidszon och formatet hämtas från användarens språkinställning.

Händelsedata från IA-systemet kan hämtas som Excel-filer eller PDF:er. Data om riskhanteringar hämtas som protokoll till PDF.

Det går inte att manipulera loggarna inifrån IA-systemet. Loggarna sparas ograverade så länge ärendet inte tas bort eller användaren raderas eller inaktiveras.

Systemet loggar ändring och läsning av händelsedata. Loggning av inloggningar görs för så väl lyckade som misslyckade försök. Behörighetsförändringar loggas också.

Tillgången till loggar är styrd via rollernas behörighet.

10.3 Säkerhetskopiering

Databaser såväl som transaktionsloggar säkerhetskopieras regelbundet, och återläsning av säkerhetskopior testas regelbundet. Systemet är anpassat för en maximal dataförlust på 1 timma (dvs RPO=1), men backup sker på transaktionslogg var 15:e minut 24/7/365.

Leverantören fokuserar på hög redundans och tillgänglighet i arkitekturen. Driftpersonal för katastrofåterställning och felsökning utom kontorstid sker enligt beredskapsrutin av egen personal. Säkerhetskopior tas på servrar i båda datorhallarna och sparas på en plats skild från originalet.

10.4 Skydd mot skadlig kod

Följande skydd har vi i trafik från Internet mot IA-systemet:

- Antivirus
- Antispyware
- Vulnerability protection (CVE-sårbarheter)
- Fileblock (Exekverbara filer kontrolleras i Sandbox)

Endast http och https-trafik är godkänd som standard. IA-systemet är avgränsat från Leverantörens övriga trafik via brandväggar.

Klienter som nyttjas för att ansluta till servrarna har antivirus-mjukvara aktiv. Såväl servrar som klienter härdas innan driftsättning.

10.5 Sårbarhetshantering

Dedikerad personal har som uppgift att bevaka information från leverantörer av produkter och komponenter gällande säkerhetsbrister och tillgängliga uppdateringar. En riskanalys görs varefter allvarliga säkerhetsbrister och viktiga uppdateringar hanteras omgående, och övriga hanteras enligt

dokumenterad rutin för regelbunden versionshantering. Samtliga ändringar i nyttjad mjukvara och i IA-systemet ingående tredjepartskomponenter dokumenteras.

11 Kommunikationssäkerhet

Lösningen skyddas med en brandvägg så att endast fördefinierad trafik ges nätverksåtkomst till lösningen. Det innebär att webbserver och databasserver ligger i Leverantörens DMZ som är skilt från interna nät och Internet.

All trafik som passerar brandväggen loggas. Loggarna sparas 12 månader bakåt i tiden, alla poster sparas lika länge.

12 Anskaffning, utveckling och underhåll av system

12.1 Test och utveckling

Utvecklingsteam

Systemutveckling sker agilt som bygger på proaktiv kvalitetssäkring med kontinuerlig testning och återkoppling av resultat. Systemutveckling inom agil utveckling omfattar både kravarbete och test.

Utvecklingsteamet ansvarar gemensamt för alla aktiviteter som krävs för att kvalitetssäkra varje PBI (product backlog item) i varje sprint. Teamet är också ansvariga för IA-systemets och produktens långsiktiga kvalitetssäkring.

Referensgrupp

Önskemål om ny funktionalitet hanteras via en referensgrupp. Referensgruppen består av företagsrepresentanter som utses av branscherna plus branschföreträdare. Referensgruppen samlas två gånger per år och har till uppgift att prioritera dessa önskemål. För att få bereda ärenden finns det olika utskott vars uppgift är att lägga fram konkreta idéer för nya lösningar gällande olika områden. Utskotten består av användare från olika företag och branscher med intresse för specifika frågor. Utskotten används också som bollplank i utvecklingsarbetet för att Leverantören ska kunna stämma av att lösningen blir som referensgruppen önskar.

Information om innehåll i kommande releaser skickas en vecka före produktionssättning till respektive företags huvudadministratörer.

IT-miljöer

Separata IT-miljöer används för produktion respektive test och utveckling av IA-systemet.

Produktionsdata används inte i utvecklings- och systemtestmiljö.

12.2 Webbläsare och verktyg

IA-systemet är anpassat för XHTML-kompatibla webbläsare. IA-systemet genererar rapporter i PDF, TIFF och Excel, samt använder Google Maps för kartfunktion.

Användning av Google Maps innebär godkännande av Googles användarvillkor: https://maps.google.com/help/terms_maps/ och Privacy policy https://www.google.com/policies/privacy/. När kartan öppnas förs inga uppgifter över till Google från IA-systemet.

Om ni inte önskar använda Google Maps kan ni stänga av funktionen under Generella inställningar på sidan Admin/Organisation i systemet.

12.3 Penetrationstester

Utförliga penetrationstester av systemets säkerhet görs av externa partners minst en gång per år. Användarföretag får ej genomföra en säkerhetsgranskning eller penetrationstest av IA-systemet utan att detta först godkänts av Leverantören. Kontakta Leverantörens IA-support för vidare information.

12.4 Avveckling

Efter avtalets upphörande och, i enlighet med de allmänna villkoren, kommer personuppgifter raderas på inrapporterade arbetsskaderisker och arbetsskador, övriga händelser raderas.

I det fall användarföretaget önskar få sina data migrerad kan data om inrapporterade händelser hämtas ut till Excel, data om inrapporterade riskhanteringar hämtas som protokoll till PDF.

13 Hantering av informationssäkerhetsincidenter

Applikationsansvarig leder det operativa arbetet med hanteringen av allvarliga IT-incidenter, vilket innebär kommunikation, utredning och rapportering.

Applikationsansvarig analyserar IT-incidenterna för att säkerställa att tillräckliga åtgärder har vidtagits för att hantera incidenten samt för att verksamheten ska kunna utnyttja erfarenheterna av dessa i den operativa riskhanteringen.

En lösningsgrupp tillsätts för att lösa incidenten samt bistå applikationsansvarig med utredningsarbetet.

I det fall AFA Försäkring utsätts för en cyberattack aktiveras företagets egen CERT.

Beroende på omfattningens allvarlighetsgrad av incidenten kan Leverantörens krisledningsorganisation aktiveras.

Hantering av personuppgiftsrelaterade incidenter hanteras i enlighet med Personuppgiftsbiträdesavtalet.

14 Kontinuitetshantering

IA-systemet är speglat i två separata datorhallar inom Stockholmsområdet. Vardera datorhall är dimensionerad för att kunna upprätthålla systemets tillgänglighet om en av datorhallarna blir otillgänglig.

15 Efterlevnad

Internrevisionen hos Leverantören arbetar enligt en årligen fastställd revisionsplan. Rapportering sker till styrelsen, revisionsutskott, och VD. Revisionsplanen upprättas genom en objektiv och oberoende granskning utifrån väsentlighet och risk för att ge en helhetsbedömning av verksamhetens interna styrning och kontroll.