DATASÄKERHETEN PÅ UNIVERSITETSANSOKAN.FI-TJÄNSTEN

I förverkligandet av datasäkerheten på universitetsansokan.fi-tjänsten har datasäkerhetsanvisningar givna av ledningsgruppen för datasäkerheten inom statsförvaltningen samt principerna för planering och förverkligande av den offentliga förvaltningens nättjänster följts. På detta sätt har man i konstruktionen av tjänsten i enlighet med datasäkerhetsanvisningarna strävat efter att nå en så hög datasäkerhetsnivå som möjligt.

Identifikation av tjänsten och kunden

I tjänsten används sådana certifikattjänster att kunden inte behöver ifrågasätta deras tillförlitlighet. Identifikationen av tjänsten förutsätter en certifikattjänst i en servermaskin. Tjänsten används med en krypterad förbindelse (SSL), som kontrollerar att certifikattjänsten som används är beviljad av en certifikattjänst som kunden godkänt och att den är ämnad för serveradressen i fråga. Kunden behöver identifiera sig endast då hon använder vissa tjänster som ingår i systemet eftersom principen för datasäkerhetsanvisningarna är att kundidentifikationen endast görs vid behov. Av kunden krävs en sådan version av webbläsaren som datasäker användning av tjänsten förutsätter.

Användbarhet och informationens helhet

Nödvändigheten av uppgifterna som frågas av kunden har utvärderats i förhållande till användningsändamålet. Inget sådant frågas, som inte behövs i en ansökan till universitetsutbildning. På ansökningsblanketten ges endast aktuell information, eftersom ansökningsblanketten genereras från realtidsuppgifter som finns uppdaterade i databasen. Kontrollen av blankettens uppgifter görs omedelbart efter att uppgifterna matats in och efter att uppgifterna mottagits visas en kvitteringsanmälan åt kunden.

Webbläsaren lagrar sidor som kunden använt på arbetsstationens skiva för eventuell återanvändning av sidorna. På så sätt behöver de inte (till alla delar) sökas på nytt från den ursprungliga adressen. Mellanminnet kan vara en datasäkerhetsrisk i datorer som är i gemensam användning. I tjänsten får kunden anvisningar för tömning av minnet om systemet används av många användare i en och samma maskin.

Kunden erbjuds omfattande anvisningar för användning av tjänsten och tillgång till ytterligare information på Studieinfo-sidorna, som upprätthålls av Utbildningsstyrelsen. På tjänstens webbplats finns en länk till registerbeskrivningen där kunden informeras om rätten att kontrollera uppgifter i enlighet med personuppgiftslagen.

Ett separat tillstånd att överlåta namn och adressuppgifter bes av kunden. Registreringsbeskrivningen är en del av anvisningarna. På tjänstens webbplats för anvisningar finns en länk till den tekniska datasäkerhetsbeskrivningen, där kunden informeras om användningen av en krypterad förbindelse.

Överföring av uppgifter

Uppgifterna, som kunden lagrat i systemet, är konfidentiella och de överförs till tjänsten med en krypterad förbindelse (lösningen är SSL). I datasäkerhetsanvisningarna rekommenderas att kryptering används vid

Opetushallitus
Hakaniemenranta 6, PL 380, 00531 Helsinki, puhelin 040 348 7555, faksi 040 348 7865, etunimi.sukunimi@oph.fi, www.oph.fi
Utbildningsstyrelsen
Hagnäskajen 6, PB 380, 00531 Helsingfors, telefon 040 348 7555, fax 040 348 7865, fornamn.efternamn@oph.fi, www.oph.fi

överföring av uppgifter på internet även om överföringen gäller endast informativa www-sidor. Särskild uppmärksamhet har fästs vid säkerheten mellan länkarna för tjänstesystemet och bakgrundssystemet och de har konstruerats så att systemen har separerats från varandra.

Den elektroniska tjänstens kunder har endast tillgång till uppgifter som är tillåtna för dem.

Applikationsarkitektur

Applikationsarkitekturen baserar sig på en komponentbaserad multinivåarkitektur. Komponenterna och nivåerna förmedlar information till varandra med servicebegäran där källan för begäran och innehållet kontrolleras innan begäran besvaras. T.ex. servicebegäran som kommer från tjänstesystemet till grundsystemet har noggrant begränsats till sådana som specificerats på förhand. En del av de för säkerheten centrala funktionerna har separerats till egna komponenter, som de övriga komponenterna använder.

DATASÄKERHETSLÖSNINGAR

Då infrastrukturen för Webbansökningstjänster (www.universitetsansokan.fi, www.studieval.fi, www.-yhansokan.fi, www.opekorkeahaku.fi och www.admissions.fi), som upprätthålls av Utbildningsstyrelsen har konstruerats, har finansministeriets användnings- och säkerhetsrekommendationer för internet beaktats. Rekommendationerna beskriver säkerhetsförutsättningar för internetanvändning.

Nätets struktur

I informationssystem hålls verksamhet som sker genom det offentliga nätet noggrant avskiljt från verksamheten i organisationens eget nät. Www-värddatorerna är placerade utanför det interna nätet och ur dem har endast nödvändig telekommunikation till organisationens informationssystem öppnats i brandmurarna.

Serviceområde

Det tekniska serviceområdet har dubblerats för alla kritiska komponenters del. Internetanslutningarna har förverkligats genom två olika operatörer, alla aktiva telekommunikationsanordningar i anknytning till området (router och kopplingar) brandmurar, SSL-acceleratorer och applikationens värddatorer är dubblerade. Applikationens värddatorer finns på ett s.k. DMZ-område, som planerats för internetbruk och databasservern finns bakom brandmuren i ett annat nätverk. Alla anslutningar till och från det skyddade nätet går via brandmuren och de anslutningar som får passera specificeras i brandmuren.

Trafiken från internet routas till applikationservrarna via en lastbalanseringstjänst.

Applikationen kräver en skyddad trafikeringsmetod, så applikationens servicekallelser tvingas av lastbalanseraren till användning av SSL med en redirect-funktion. I serviceområdet finns SSL-accelerationsanordningar, som har som uppgift att ändra den krypterade https-trafiken till http-trafik.