Tjänsteutlåtande
Utfärdat 2024-06-03
Diarienummer 0193/24

Handläggare
Nicholas Öfwerman
E-post: nicholas.ofwerman@intraservice.goteborg.se

Tjänsteutlåtande - Anvisning för autentisering och åtkomst

Förslag till beslut

I nämnden för Intraservice:

Intraservices anvisning för autentisering och åtkomst fastställs.

Sammanfattning

Kommunfullmäktige fastställde i maj 2023 stadens riktlinjer för informationssäkerhet. I riktlinjens kravställning framgår bland annat att nämnder och styrelser ska säkerställa att åtkomst och behörighet till information ges restriktivt utifrån arbetsuppgifter och organisatorisk tillhörighet, samt att åtkomst till information bygger på personliga användaridentiteter och är spårbar till en fysisk person. Vidare ska nämnder och styrelser säkerställa att autentisering och åtkomstkontroll till administratörs- och systemkonton sker med unika lösenord och baseras på flerfaktorsautentisering.

Den nya cybersäkerhetslagen, baserad på NIS2-direktivet, kräver också strategier för åtkomstkontroll och tillgångsförvaltning, säkrade lösningar för kommunikation, och lösningar för autentisering, där autentisering syftar till användning av multifaktorautentisering eller kontinuerlig autentisering som en del av riskhantering.

Göteborgs Stads riktlinje för informationssäkerhet fastställer även att Göteborgs Stads verksamheter är beroende av ett fungerande nätverk och Reglemente för Göteborgs Stads nämnd för Intraservice §4 fastställer ansvaret för nämnden att leverera, förvalta och vid behov utveckla digital infrastruktur åt stadens nämnder och styrelser, vilket innefattar upprätthållande av en effektiv digital infrastruktur där krav utifrån informationssäkerhet och gällande lagstiftning är säkerställda. För att förhindra obehörig åtkomst till nätverk och anslutna tjänster ska det finnas säkerhetsåtgärder på plats för att säkerställa konfidentialitet och riktighet för information som överförs. Detsamma gäller för att upprätthålla tillgänglighet till nätverkets tjänster.

Kommentar [EÖ1]: kan kanske vara värt att nämna att det även ingår i vårt grunduppdrag i reglementet att tillhandahålla säker IT-infrastruktur

Kommentar [NÖ2R2]: åtgärdat

Informationsklassning utgör tillsammans med riskanalyser kravställningen för de säkerhetsåtgärder som ska tillämpas på Intraservices information. Två av dessa säkerhetsåtgärder är autentisering och åtkomst, där autentiseringen verifierar identiteten och åtkomst styr vilken information identiteten har tillgång till. Detta gäller samtliga identiteter, såväl anställda, konsulter, politiker, leverantörer och medborgare som externa användare, tex elever eller medborgare.

Syftet är att skydda Intraservices information från obehörig åtkomst. Bristfällig efterlevnad av kravställda autentiseringsmekanismer och åtkomstkontroller kan resultera i att informationen får ett otillräckligt skydd och att dataläckage kan ske ohindrat.

Förvaltningen bedömer därför att nämnden för Intraservice bör fastställa Anvisning för autentisering och åtkomst med mål att säkerställa införande av erforderliga mekanismer enligt internationella och nationella standarder för att utgöra den del av det säkerhetshöjande arbete som krävs för att upprätthålla systematisk informationssäkerhet inom Intraservice kring specifikt autentisering och åtkomst.

Bedömning ur ekonomisk dimension

I Göteborgs Stads riktlinjer för informationssäkerhet framgår att identiteter ska autentiseras samt att åtkomst och behörighet ges restriktivt. Autentiseringskraven ska följa de krav som ställs av informationstillgångarnas skyddsvärde utifrån konfidentialitet, riktighet och tillgänglighet. Förvaltningen bedömer att mekanismerna och verktygen finns utifrån ett tekniskt perspektiv, men att dom inte har verkställts inom alla tjänster där behovet finns. Ett första steg är att kartlägga informationstillgångarnas klassning, vilket ger ett skyddsvärde och därefter säkerställa att autentiseringsmekanismerna möter kraven ställda utifrån skyddsvärdet.

Förvaltningen bedömer viss kostnadsökning kopplat till ett bredare införande och förvaltning av eID. Den ökade kostnaden kommer följa den kravställning på säkerhetsåtgärder som kopplas till säkerhetsnivåerna i Göteborgs Stads informationsklassningsmodell. Ett förstärkt autentiseringsskydd kommer även innebära förändringar i fjärråtkomsttjänster som används vid arbete utanför kontoret då en autentisering kommer krävas för att aktivera fjärråtkomst.

Åtgärderna förväntas stärka säkerheten för Intraservices och Stadens information avsevärt vilket sannolikt kommer leda till betydande kostnadsbesparingar över tid. Autentisering och åtkomst är grundläggande komponenter för att skydda information utifrån dess skyddsvärde, vilket kommer vara en kravställning vid införandet av den nya cybersäkerhetslagen. Förvaltningen bedömer att en av åtgärderna för att undvika att påföras en administrativ avgift i samband med tillsyn är att införa en övergripande strategi för autentisering och åtkomst.

Kontrafaktiska kostnadsbesparingar är svårbedömda, men med en ökad informationssäkerhet minskar risken för kostsamma säkerhetsrelaterade händelser så som kapade konton, utpressningsattacker (ransomware), dataläckage, dataförlust, mm.

Bedömning ur ekologisk dimension

Förvaltningen har inte funnit några särskilda aspekter på frågan utifrån denna dimension

Bedömning ur social dimension

En standardiserad modell för autentisering och åtkomst hjälper förvaltningen styra och säkra åtkomst till information med särskilt skyddsvärde. För den enskilde innebär det sannolikt ett förhöjt skydd för känsliga personuppgifter och den personliga integriteten, samt trygghet i att veta att information är skyddad från olovlig åtkomst, förstörelse, förvanskning eller förändring.

En central aspekt kring autentisering och åtkomst är fastställande av att identiteten och dess åtkomstbehörighet är i linje med informationstillgångarnas skyddsnivåer. Förvaltningen bedömer därför att åtgärden kommer stärka arbetet med Agenda 2030 kopplat till mål 16.10 *Säkerställa allmän tillgång till information och skydda grundläggande friheter.* Förvaltningen bedömer att förhöjd säkerhet genom starkare autentiseringsmekanismer och åtkomstkontroll kommer stärka skyddet för den information som behövs för att upprätthålla kritiska samhällstjänster som bedrivs i kommunal regi och kommer därför även stärka mål 11B *Utveckla strategier för inkludering, resurseffektivitet och katastrofriskreducering.*

Samverkan

Samverkan har skett 2024-05-23.

Bilagor

1. Nämnden för Intraservice anvisning för autentisering och åtkomst

Ärendet

Föreslagen anvisning ska utifrån Göteborgs Stads riktlinje för informationssäkerhet ange hur Intraservice ska implementera autentisering och åtkomst. Anvisningen ska säkerställa att Intraservice har korrekta metoder och verktyg för att säkerställa att identiteter fastställs innan de får åtkomst till information eller informationsbärare enligt de krav som informationsklassningen ställer.

Beskrivning av ärendet

Bakgrund

Kommunfullmäktige fastställde i maj 2023 stadens riktlinjer för informationssäkerhet. I riktlinjens kravställning framgår bland annat att Nämnder och styrelser ansvarar för att:

> *- säkerställa att åtkomst och behörighet till information ges restriktivt utifrån arbetsuppgifter och organisatorisk tillhörighet*
>
> *- säkerställa att behörigheter följs upp vid behov. Vid byte eller förändring av tjänst ska behörigheter och åtkomst till information ses över*
>
> *- säkerställa att åtkomst till information bygger på personliga användaridentiteter och är spårbar till en fysisk person*
>
> *- säkerställa att autentisering och åtkomstkontroll till administratörs- och systemkonton sker med unika lösenord och baseras på flerfaktorsautentisering*
>
> *- säkerställa att regelverk och rutin för registrering och avregistrering av behörigheter fastställs innan system tas i bruk.*

Autentisering har som syfte att verifiera identiteten på en användare eller enhet som försöker få tillgång till ett system, vanligtvis genom att användaren tillhandahåller bevis på sin identitet, såsom ett användarnamn och lösenord, biometrisk information (fingeravtryck, ansiktsigenkänning), eller tvåfaktorsautentisering (en kombination av något användaren vet och något användaren har). Autentisering handlar om att bekräfta identiteten på användaren eller enheten. Det svarar på frågan "Vem är du?"

Åtkomst har som syfte att bestämma vilken nivå av tillgång en autentiserad användare eller enhet har till resurser i systemet genom att kontrollera och begränsa vad den verifierade användaren kan göra eller se efter att de har autentiserats. Åtkomstkontroll kan baseras på olika faktorer såsom användarroller, behörighetsnivåer, och specifika tekniska policyer. Åtkomst handlar om att ge eller begränsa tillgång till resurser baserat på den bekräftade identiteten. Det svarar på frågan "Vad får du göra?"

Genom att kombinera dessa två processer kan system säkerställa att endast rätt användare får tillgång till rätt resurser på ett säkert sätt.

Som grund till detta ligger även informationsklassning som fastställer skyddsnivåer utifrån konfidentialitet, riktighet och tillgänglighet.

- Konfidentialitet: att information inte tillgängliggörs eller avslöjas för obehöriga
- Riktighet: att informationen skyddas mot oönskad förändring, att information är korrekt och inte manipulerad eller förstörd

- Tillgänglighet: att information är tillgänglig och användbar när den behövs

Informationsmängderna blir tilldelade ett värde mellan 0–4 för aspekterna konfidentialitet, riktighet och tillgänglighet respektive. En given informationsmängd kan ha högt värde för konfidentialitet men inte för riktighet och tillgänglighet och tilldelas då konfidentialitet 3, riktighet 1 och tillgänglighet 1.

För att riktlinjen för informationssäkerhet ska kunna efterlevas i praktiken krävs det ytterligare styrning i nämnden i syfte att konkretisera att autentisering och åtkomst behöver följa de säkerhetskrav som informationsmängderna ställer utifrån sin informationsklassning; Ju högre informationsklass, desto högre autentiseringskrav. Detta är särskilt viktigt med tanke på NIS-2[1] direktivet som träder i kraft 2024–10 och översätts i cybersäkerhetslagen som gäller från 2025–01.

NIS2 syftar till att stärka cybersäkerheten i Europa genom att införa strängare krav på medlemsstater och företag inom kritiska sektorer. Även om NIS2 inte specificerar tekniska detaljer, innebär kraven på högre säkerhetsåtgärder att företag, myndigheter och organisationer inom direktivets tillämpningsområde kommer att behöva:

- Implementera multifaktorautentisering (MFA) för att stärka inloggningsprocessen
- Använda starka lösenordspolicyer
- Tillhandahålla utbildning för anställda om vikten av säker autentisering
- Säkerställa att autentiseringslösningar uppfyller aktuella säkerhetsstandarder och riktlinjer från relevanta myndigheter och branschorgan

DIGG[2] har redan granskat och validerat ett flertal mekanismer för autentisering enligt tillitsnivåerna som motsvarar informationsmängdernas klassningsnivåer, och detta tillitsramverk bör Intraservice luta sig mot i sitt arbete med autentisering.

Nuvarande modell

Nuvarande modell för autentisering utgår från Göteborg Stads riktlinje för informationssäkerhet vilken endast specificerar flerfaktorsautentisering för åtkomst till administratörs- och systemkonton, och idag saknas en anvisning inom Intraservice som förtydligar hur detta ska efterlevas inom förvaltningen. Anvisningen pekar på vikten av autentisering för åtkomst till informationsmängder i sin helhet för att nämnden ska leva upp till de krav som ställs i NIS2.

Autentisering till priviligierade system tillämpas genom flerfaktorsautentisering, även om det inte finns en anvisning eller instruktion som har fastställt vad och hur det ska utföras. Övrig autentisering sker med en faktor, dvs användarnamn och lösenord.

Efter identiteten är autentiserad har användaren åtkomst till trådlöst nät vid arbete på kontoret via kontroll av certifikatet som finns på klienten. Men om användaren arbetar

[1] NIS-2 (Network and Information Systems Directive 2) är ett EU-direktiv med syfte att stärka cybersäkerheten inom sektorer som är kritiska för samhällsfunktionen.
[2] DIGG (Myndigheten för digital förvaltning) är en myndighet som lyder under Finansdepartementet och vars uppdrag är att stödja och samordna den förvaltningsgemensamma digitaliseringen i Sverige.

hemifrån, ansluts denne via VPN utan autentisering och certifikatet på klienten används även här, trots att det inte autentiserar identiteten och endast maskinen.

Därefter har användaren åtkomst till produktionsnätet samt alla resurser och informationstillgångar som rollen definierar. Med andra ord blir tillitsnivån till information inte högre än klass 1 då det endast sker autentisering med en faktor.

Externa användare berörs av samma krav kring autentisering, och det baseras på skyddsvärdet på informationen den externa användaren behöver åtkomst till. Även i det fallet ska Intraservice luta sig mot de tillitsramverk som godkänts av DIGG.

Föreslagen modell

Modellen består av ett styrdokument som efterföljs av stödjande instruktioner och rutiner:

- Nämnden för Intraservices anvisning för autentisering och åtkomst.
  Anvisningen utgår från principen om minsta möjliga tillgång där konton tilldelas endast åtkomst till den information dom behöver för att utföra sina uppgifter och roller samt att autentisering ska ske enligt godkända tillitsramverk och i nivå med informationsklassen på informationen man behöver åtkomst till.

Målsättningen med autentiseringskraven enligt NIS2-direktivet är att stärka säkerheten och motståndskraften hos nätverk och informationssystem genom att säkerställa att endast behöriga användare får tillgång till kritiska system och information.

När identiteten väl är autentiserad enligt korrekt protokoll kan anslutning till det trådlösa nätet på kontoret med befintligt klientcertifikat eftersom man samtidigt kan utgå från att användaren har identifierat sig för att få åtkomst till lokalen. Vid arbete hemifrån ska fjärranslutning initieras genom ytterligare en faktor, där certifikatet på klienten inte är en giltig identifikator för identiteten.

Förhållandet mellan autentisering, anslutning och åtkomst är centralt inom informationssäkerhet och hantering av digitala resurser:

- Autentisering - *Första steget i säkerhetsprocessen som bekräftar användarens identitet.*
  Autentisering är processen för att verifiera identiteten på en användare eller enhet som försöker få tillgång till ett system eller en resurs. Syftet är att säkerställa att användaren är den som den utger sig för att vara. Metoder som kan användas är tex lösenord, biometriska data (t.ex. fingeravtryck eller ansiktsigenkänning), multifaktorsautentisering, eID eller säkerhetstokens. När en användare loggar in på ett system med minst användarnamn och lösenord, bekräftas identiteten genom autentisering.
- Anslutning - *Nästa steg efter framgångsrik autentisering. Etablerar en säker kommunikationskanal mellan användaren och systemet, och kan ske parallellt med autentisering, särskilt i webb- och nätverksmiljöer.*
  Anslutning innebär etableringen av en länk mellan en användares enhet och ett system eller en nätverksresurs efter att autentiseringen har lyckats. Syftet är att skapa en säker kommunikationskanal för interaktion med systemet. Metoder som kan användas är tex VPN (Virtual Private Network), VDI (Virtual Desktop Interface) och SSL/TLS (Secure Sockets Layer/Transport Layer Security) för

säkra webbanslutningar. Efter en användare har autentiserats via en klient för fjärråtkomst skapas en säker anslutning till Stadens nätverk.

- Åtkomst - *Sista steget som bygger på framgångsrik autentisering och anslutning. Bestämmer vad användaren har rätt att göra inom systemet och baseras på användarens identitet och tillhörande behörigheter.*
  Åtkomst handlar om att bestämma vilka resurser och data en autentiserad användare har rätt att använda eller se. Syftet är att kontrollera och begränsa användarens aktiviteter och tillgång till systemresurser baserat på identitet och roll. Metoder som kan användas är tex rollbaserad åtkomstkontroll (RBAC), attributbaserad åtkomstkontroll (ABAC) och policybaserade kontroller. En användare som har autentiserats och anslutit till ett nätverk kan ha rätt att läsa vissa filer men inte att redigera eller radera dem beroende på deras behörighetsnivå.

Sammanfattningsvis verifieras användaren, en säker kanal för kommunikation etableras och därefter får användaren tillgång till de resurser som den ska ha tillgång till. Tillsammans utgör dessa tre steg en säkerhetsram som skyddar system och information från obehörig åtkomst och manipulation.

Målsättningen med autentisering och åtkomst är att efterfölja arbetet med den nya informationsklassningsmodellen för att säkerställa att endast autentiserade identiteter får åtkomst till rätt information vid rätt tillfälle och därmed ytterligare stärka skalskyddet till samtliga informationstillgångar, inte bara system- och administratörskonton.

Reglerad kravställning

Kravställning på informationssäkerhet har sitt ursprung inte endast i verksamhetens bedömning av värdet utan kan i många fall vara uttryckt i lagstiftning eller styrdokument. Det är viktigt att man identifierar informationsklass på information som finns i processer och informationsbärare för att fastställa vilka tillitsnivåer som behöver implementeras för att autentisera en identitet som ska ha åtkomst till informationen.

De specifika målen med autentiseringskraven under NIS2 är:

- Förhindra obehörig åtkomst:
  Genom att införa starka autentiseringsmetoder, såsom multifaktorautentisering (MFA), minimeras risken för att obehöriga användare kan få tillgång till känsliga system och information.
- Öka säkerheten för kritiska infrastrukturer:
  Många av de sektorer som omfattas av NIS2-direktivet, som energi, transport, bankväsende, hälso- och sjukvård, och digital infrastruktur är samhällskritiska. Starka autentiseringskrav bidrar till att skydda dessa sektorer mot cyberattacker.
- Minska risken för cyberattacker:
  Många cyberattacker börjar med komprometterade användaruppgifter. Genom att kräva robust autentisering minskar risken för att sådana attacker lyckas.
- Skydda personuppgifter:
  Genom att säkerställa att endast behöriga individer har tillgång till system och information, skyddas personuppgifter och annan känslig information mot obehörig åtkomst och potentiella dataintrång.

- Stärka incidentrespons och återhämtning:
  Starka autentiseringsåtgärder bidrar till snabbare och mer effektiv identifiering av säkerhetsincidenter, vilket underlättar en snabb respons och återhämtning.
- Öka förtroendet för digitala tjänster:
  Genom att implementera starka säkerhetsåtgärder, inklusive autentisering, ökar förtroendet för digitala tjänster och nätverk, vilket är avgörande för ekonomisk tillväxt och säker digitalisering.

Sammanfattningsvis syftar autentiseringskraven enligt NIS2-direktivet till att förbättra den övergripande säkerheten och motståndskraften hos nätverk och informationsbärare. Genom att säkerställa att endast behöriga användare kan få tillgång till känsliga system och data, minskar risken för cyberattacker, kritisk infrastruktur och personuppgifter skyddas och förtroendet för digitala tjänster ökar. Detta är avgörande för att upprätthålla samhällsfunktioner och säkerhet i en alltmer digitaliserad värld.

Delegering av mandat att fastställa rutin och instruktion

Förvaltningen bedömer att tidigare brist på anvisningar för autentisering och åtkomst är oförenligt med kraven som NIS2 ställer. Det finns mekanismer och verktyg för att implementera tillräcklig autentisering där det behövs, men det har inte gjorts på bred front. För att lyckas implementera korrekta autentiseringsprotokoll inom förvaltningen behöver rutiner och instruktioner tas fram i och med att skydden appliceras i en utrullningstakt som är görbar. Dessa ska tas fram i samråd mellan de enheter som ansvarar för olika delar i den sammanvävda processen Autentisering-Anslutning-Åtkomst med syfte att skydda alla informationsmängder på korrekt sätt, och inte enbart system- och administratörskonton.

Med detaljeringsnivån och eventuella ekonomisk påverkan följer ett behov av återkommande aktualisering av rutinen och instruktionen; det framstår som onödigt betungande för både förvaltningen och nämnden att återkommande lyfta mindre förändringar i dessa stödjande dokument. Förvaltningen föreslår därför att Nämnden för Intraservices CISO delegeras att fastställa förändringar i rutiner och instruktioner kopplade till anvisningen.

Förvaltningens bedömning

Autentisering och åtkomst utgör ett starkt skydd för den information en användare ska få tillgång till, baserat på informationens informationsklassning. Anvisningen lutar mot tillitsramverk som är fastställda och godkända av DIGG, vilket innebär följsamhet mot nationell standard.

Initiativ kring starkare lösenordskrav är bra, men dom löser inte grundproblemet med autentiseringen. Där autentisering sker med endast användarnamn och lösenord (enfaktorsautentisering) är givetvis ett starkare lösenord bra, men även ett starkt lösenord kan kompromitteras. Enfaktorsautentiseringar är dessutom dom som är enklast att angripa och exploatera vid nätfiske, och då är styrkan på lösenordet oviktigt – det enda som skyddar är flerfaktorsautentisering.

Bristfällig efterlevnad mot de krav som NIS2 ställer på autentisering och åtkomst i förhållande till klassningen av informationsmängderna kan resultera i otillbörlig åtkomst till känslig information eller informationsbärare.

Intraservice är Stadens centrala leverantör av digital infrastruktur och digitala tjänster och hanterar därmed information som är av stor vikt inte bara för myndigheten själv utan för Staden som helhet. Det är förvaltningens bedömning att en anvisning som pekar mot vedertagna standarder för autentisering och åtkomst gynnar både Intraservice och Staden i informationssäkerhetsarbetet, skyddar information från otillbörlig åtkomst och i förlängningen även Stadens möjlighet att leverera trygga och säkra tjänster till medborgarna.

Utan en standardiserad modell för autentisering och åtkomst riskerar Intraservice att ha svårt att uppfylla kraven i kommande cybersäkerhetslagstiftning (NIS2-direktivet).

Behovet av styrning och förtydligande på nämndnivå är angelägen med tanke på Intraservices särställning som tjänsteleverantör till övriga Staden. Det blir därför viktigt att kunna särskilja på den information som Intraservice hanterar åt andra och därför inte är informationsägare av och den information som Intraservice själv innehar informationsägarskap för. Verktygen för erforderlig autentisering och åtkomst ska erbjudas från Intraservice och kunna appliceras av alla kunder som Intraservice levererar drift eller tjänster till.

För att säkerställa att autentiseringsmetoder sker på ett likartat sätt inom förvaltningen är det nödvändigt att utarbeta detaljerade rutiner för hur det ska genomföras och rullas ut på de informationsbärare eller tjänster som kräver det. En hög detaljeringsgrad i rutiner för genomförandet leder till att bestämmelserna periodvis behöver förändras i syfte att vara uppdaterade med systemstöd, lagar, styrdokument etcetera

Förvaltningen bedömer därför att nämnden bör fördela mandat att fastställa detaljerade rutiner och instruktioner för informationsklassningens genomförande till Intraservices CISO.

Stina Hall Hellqvist	Peter Söderström
Avdelningschef	Förvaltningsdirektör