Risk- och sårbarhetsanalys

2025-11-14

Hos Stockholm Vatten och Avfall

Sammanfattning

Denna risk- och sårbarhetsanalys är framtagen åt Stockholm Vatten och Avfall på uppdrag av IT-säkerhetschefen. Analysen genomförs för att uppfylla NIS2-direktivets krav på riskhantering enligt kommande cybersäkerhetslag samt GDPR Artikel 32 krav på lämpliga säkerhetsåtgärder.

Stockholm Vatten och Avfall är en kommunal förvaltning som ansvarar för samhällskritisk infrastruktur i Stockholmsregionen. Verksamheten omfattar dricksvattenproduktion och distribution till 1,6 miljoner människor, avloppsrening för 1,2 miljoner människor, samt avfallshantering för 1 miljon stockholmare med 8 miljoner tömningar per år.

Stockholm Vatten och Avfall omfattas av två regelverk:

Kritisk infrastruktur:

- NIS2-klassificering: väsentlig entitet enligt Artikel 3
- Sektor: dricksvatten och avlopp (Annex I, punkt 5a och 5b)
- Tillsynsmyndighet: Myndigheten för samhällsskydd och beredskap (MSB)

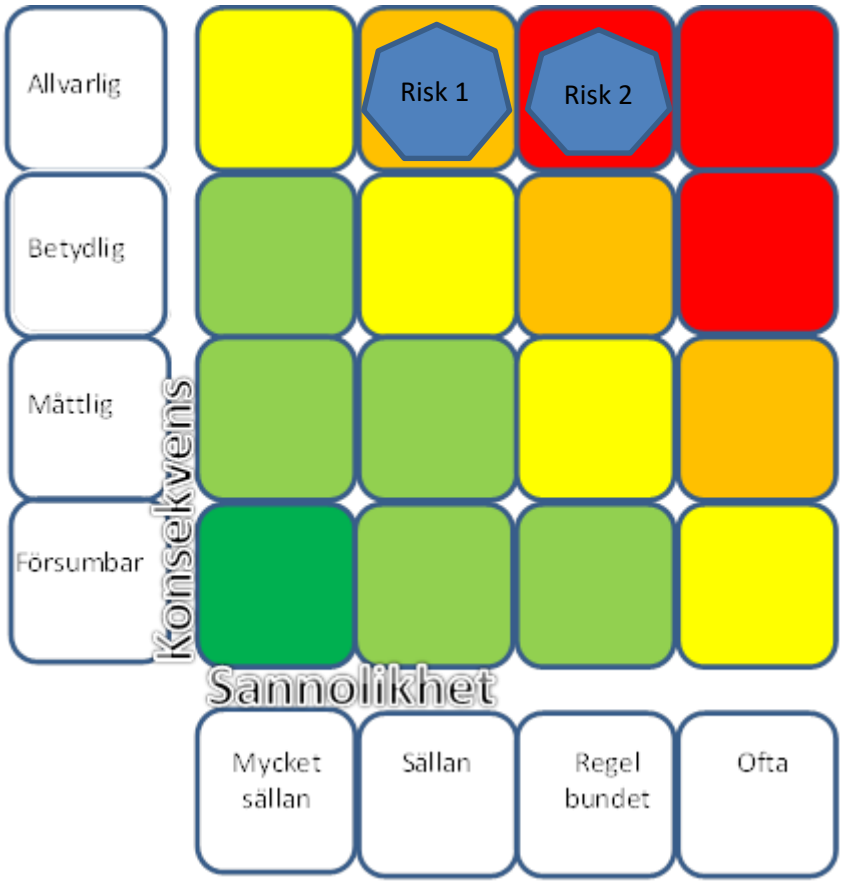
Personuppgiftsskydd:

- GDPR-status: Personuppgiftsansvarig för kund- och personaluppgifter.
- Tillsynsmyndighet: Integritetsskyddsmyndigheten (IMY)

Analysen fokuserar på två kritiska cybersäkerhetsrisker som kan påverka verksamhetens förmåga att leverera samhällskritiska tjänster och skydda personuppgifter. Analysen tar hänsyn till kommande svensk cybersäkerhetslag, MSB:s förslag till föreskrifter (MSBFS), ISO 27001 & 27002 samt GDPR.

Statistik om verksamheten är hämtad från Stockholm Vatten och Avfalls hemsida. Information om tekniska system (SCADA, servrar, etc.) är baserad på vanliga lösningar inom branschen och ska ses som exempel.

Båda identifierade risker bedöms som allvarliga och kräver åtgärder. Nuvarande skyddsnivå är otillräcklig för att uppfylla kommande NIS2-krav och GDPR:s dataskyddskrav.



Risk 1
Cyberattack mot industriella styrsystemet SCADA: en angripare tar sig in via phishing och får tillgång till SCADA-system som styr vattenproduktion. Kan manipulera kemikaliedosering vilket kan orsaka förgiftning eller vattenburen smitta hos 1,6 miljoner invånare. Kan också stoppa avloppsrening vilket leder till miljöutsläpp. Primärt en NIS2-risk med folkhälso- och miljökonsekvenser.

Risk 2
Ransomware-attack på administrativa IT-systemet: Ransomware krypterar faktureringssystem, kunddatabas och logistiksystem för sophämtning. Delar av verksamhetens kärnuppdrag upphör under viss tid och personuppgifter exponeras. Måste rapporteras till både MSB (NIS2) och IMY (GDPR). Primärt en GDPR-risk med NIS2-aspekter kring tillgång till tjänster.

Bilaga 1

Dokumentation av hot - Risk 1 Cyberangrepp mot industriellt styrsystem

Benämning

SCADA-cyberangrepp mot vattenverk

Referens till ISO 27002:
8.31 Separation of development, test and production environments
13.1 Network controls
8.7 Protection against malware

Referens till NIS2 och MSBFS:
NIS2 Artikel 21 - Cybersäkerhetsriskhanteringsåtgärder
MSBFS Kap 3 § 11 - Segmentering

Analysen har genomförts med hjälp av: IT-säkerhetschef och driftchef.

Beskrivning

Stockholm Vatten och Avfall driver vattenverk som producerar dricksvatten till 1,6 miljoner invånare. Vattnet tas från Mälaren och renas genom kemikalietillsats (klor och kalk) och filtrering innan det distribueras.

Systemet använder SCADA (Supervisory Control and Data Acquisition) för att övervaka och styra vattenproduktionen. SCADA-systemet består av:

- Centralserver med Windows Server 2019
- Styrdatorer som operatörer använder för att se processdata
- PLC:er (Programmable Logic Controllers) som styr pumpar och dosering av kemikalier
- Sensorer som mäter vattenkvalitet (pH, klornivå, temperatur)

SCADA-systemet är kopplat till organisationens huvudsakliga IT-nätverk för att tillåta fjärråtkomst och rapportering.

Påverkad personal: Driftoperatörer som övervakar vattenproduktion, processansvariga, IT-avdelning.

Scenario: En angripare skickar ett phishing-mail till en operatör. Operatören klickar på en länk och installerar malware på sin dator. Eftersom SCADA-nätverket är kopplat till det vanliga IT-nätverket kan angriparen ta sig vidare till SCADA-servern.

Angriparen kan då:

- Ändra kemikaliedosering leder till obrukbart vatten
- Stänga av pumpar stoppar vattenförsörjningen ute i nätet
- Ändra vad operatörerna ser på sina skärmar så de inte märker något (föreställ er Stuxnet!)

Konsekvenser

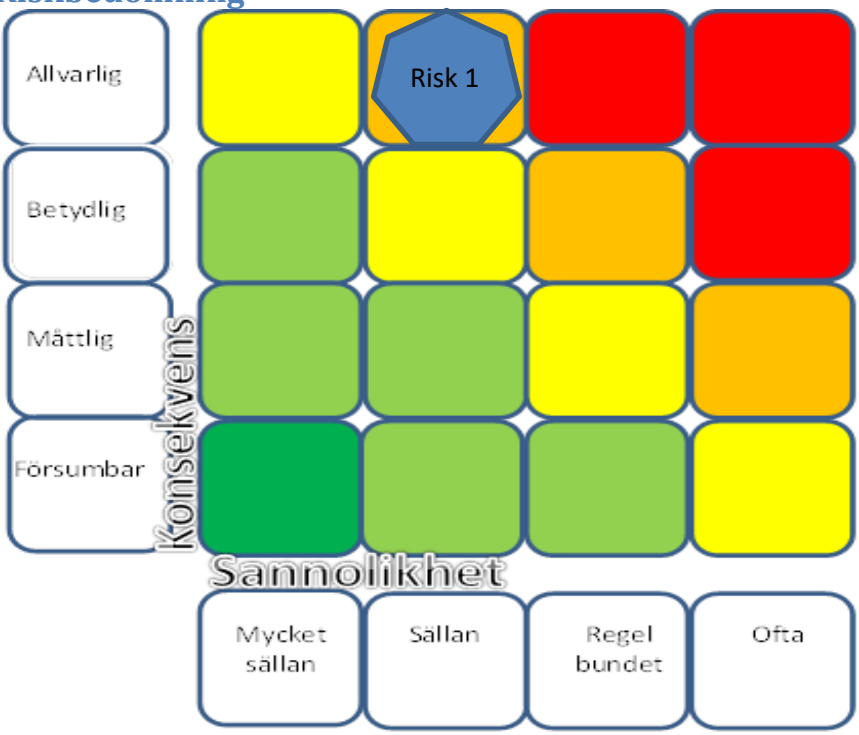
Folkhälsa och miljö: Om för mycket klor doseras kan 1,6 miljoner invånare få förgiftningssymptom. Om för lite klor doseras kan bakterier spridas i vattnet. Stockholm stad måste utfärda kokrekommendation. Om processen störs kan orenat vatten släppas ut i Mälaren.

Operativt och ekonomiskt: Vattenverken måste stängas ned för säkerhetskontroll. Återställning kan ta veckor och kostar flera miljoner kronor. Distribution av nödvatten är mycket dyrt och logistiskt svårt med tanke på antalet invånare.

Enligt NIS2: Incidenten måste rapporteras till MSB inom 24 timmar. Böter kan bli upp till 10 miljoner euro (cirka 110 miljoner SEK).

Förtroende: Media skriver negativt och förtroendet för kommunen sjunker kraftigt. Kan bli världsnyhet med tanke på omfattning.

Riskbedömning



Åtgärder

Nuvarande skydd: SCADA-nätverket är kopplat till organisationens vanliga IT-nätverk via en brandvägg. VPN finns för fjärråtkomst med användarnamn och lösenord. Windows Defender finns på SCADA-servern. Backup av SCADA-konfiguration görs ibland manuellt. Fysiskt skydd: staket, väktare och kameror vid vattenverken.

Bedömning av nuvarande skydd

Nivå	Bedömning
Det nuvarande skyddet bedöms vara tillräckligt	Nej
Det nuvarande skyddet bedöms inte vara tillräckligt, men verksamheten accepterar de kvarvarande riskerna	Nej
Det nuvarande skyddet bedöms inte vara tillräckligt, och det behövs ytterligare åtgärder	Ja

Varför nuvarande skydd inte duger: SCADA-nätverket är för nära kopplat till IT-nätverket. Om någon hackar en vanlig arbetsdator kan de ta sig vidare till SCADA. VPN saknar multifaktorsautentisering vilket gör det lättare för angripare. Windows Defender är inte anpassat för SCADA-system. Backup görs inte regelbundet vilket gör återställning svår.

Ytterligare skydd som behövs

1. **Separera SCADA från IT-nätverket**: SCADA-systemet måste isoleras bättre från vanliga IT-systemet. Installera en kraftigare brandvägg mellan nätverken som bara tillåter nödvändig kommunikation. Referens: MSBFS Kap 3 § 11.
2. **Multifaktorautentisering** (**MFA**): All fjärråtkomst till SCADA måste kräva både lösenord och en kod från mobilen. Referens: MSBFS Kap 3 § 19.
3. **Bättre övervakning av SCADA:** Installera system som upptäcker ovanliga händelser i SCADA-nätverket, till exempel om någon försöker ändra kemikaliedosering på onormala tider. Referens: MSBFS Kap 3 § 38.

4. **Regelbunden backup:** Automatisk daglig backup av alla SCADA-inställningar. Spara backup på plats som inte är kopplad till nätverket så ransomware inte kan förstöra den. Även 3-2-1-modellen är ett alternativt upplägg. Referens: MSBFS Kap 3 § 36-37.
5. **Utbildning:** Utbilda operatörer om hur phishing-attacker ser ut och varför SCADA-säkerhet är viktigt. Finns automatiserade system för detta. Referens: MSBFS Kap 2 § 11.

Dokumentation av hot - Risk 2

Benämning

Ransomware-attack på administrativa IT-system

Referens till ISO/IEC 27002:
8.7 Protection against malware
8.13 Information backup

Referens till NIS2, GDPR och MSBFS:
NIS2 Artikel 21 - Cybersäkerhetsriskhanteringsåtgärder
GDPR Artikel 32 - Säkerhet vid behandling
MSBFS Kap 3 § 36 - Säkerhetskopiering

Analysen har genomförts med hjälp av: IT-säkerhets- respektive kontorschefen.

Beskrivning

Organisationen använder flera IT-system för att hantera administration, ekonomi och sophämtningslogistik. Dessa upprätthåller personuppgifter för kunder (villaägare, bostadsrättsföreningar, företag) och anställda.

IT-miljön inkluderar:

- Windows-servrar för faktureringssystem och ekonomi
- En SQL-databas med kund- och personaluppgifter
- Logistiksystem för sophämtning
- E-postserver
- Filservrar

Påverkad personal: Administration, ekonomi, logistik, IT-avdelning.

Scenario: En anställd öppnar ett mail med en bilaga som ser legitim ut. Filen innehåller ransomware som krypterar filer på datorn och sprider sig till servrar via nätverket. Efter några timmar är följande krypterat:

- Kund- och personaldatabas
- Faktureringssystem
- Sophämtningsscheman
- E-post
- Backupper på nätverket

Angriparen kräver betalning för att dekryptera filerna.

Konsekvenser

Verksamhetspåverkan och ekonomi: Fakturering fungerar inte vilket innebär att organisationen inte får några intäkter. Sophämtning kan inte planeras

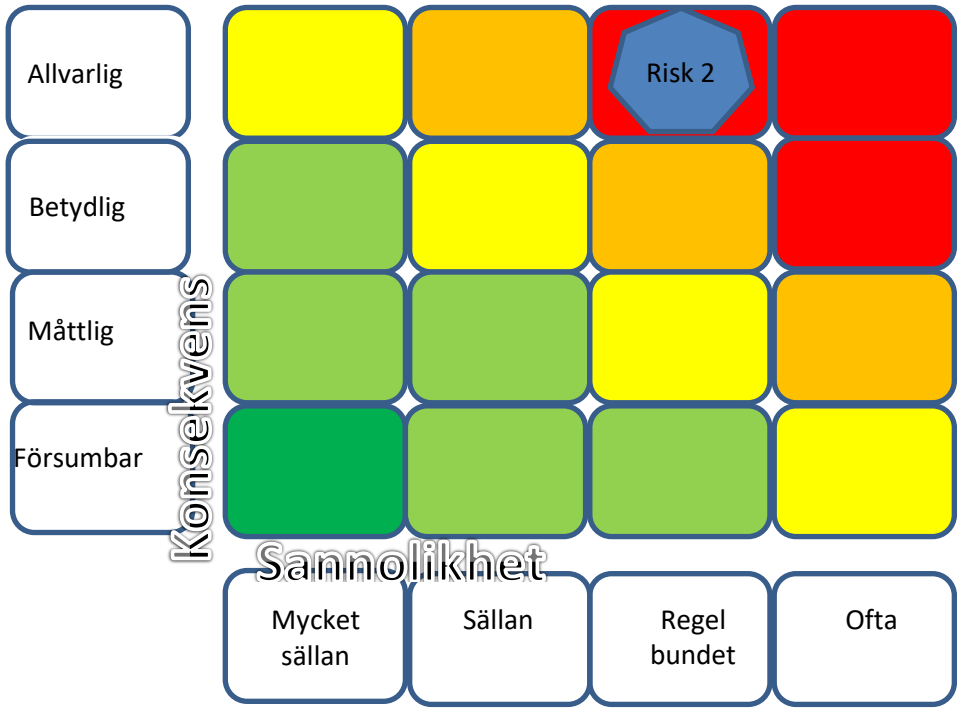
eftersom scheman är borta, vilket betyder att 1 miljon stockholmare inte får sitt avfall hämtat. Personal kan inte arbeta normalt. Återställning kan kosta flera miljoner kronor, plus eventuell lösensumma till angriparna.

Personuppgifter och GDPR: Kunddatabasen med personuppgifter är krypterad eller stulen. Detta är en personuppgiftsincident som måste rapporteras till IMY inom 72 timmar enligt GDPR Artikel 33. Böter kan bli upp till 20 miljoner euro om säkerheten bedöms vara för dålig.

Dubbel rapporteringsskyldighet: Organisationen måste rapportera till både MSB (enligt NIS2 eftersom sophämtning är en samhällskritisk tjänst) och IMY (enligt GDPR för personuppgiftsincidenten). Detta innebär mycket administrativt arbete och risk för böter från båda myndigheterna. NIS2-böter kan bli upp till 10 miljoner euro.

Samhällspåverkan och förtroende: När sophämtning inte fungerar skapar det sanitära problem och mycket klagomål från stockholmare. Media kommer att skriva negativt om händelsen vilket skadar förtroendet för kommunen. Det kan ta veckor att återställa verksamheten utan fungerande backup.

Riskbedömning



Åtgärder

Nuvarande skydd

Windows Defender på datorer och servrar. E-postserver har spam-filter. Backup görs varje vecka och lagras på nätverksansluten NAS. Brandväggar mot internet. Finns plan för incidenthantering.

Bedömning av nuvarande skydd

Nivå	Bedömning
Det nuvarande skyddet bedöms vara tillräckligt	Nej
Det nuvarande skyddet bedöms inte vara tillräckligt, men verksamheten accepterar de kvarvarande riskerna	Nej
Det nuvarande skyddet bedöms inte vara tillräckligt, och det behövs ytterligare åtgärder	Ja

Varför nuvarande skydd inte räcker:
Spam-filter fångar inte alla skadliga mail. Windows Defender kan inte stoppa ny ransomware. Backup görs för sällan (veckovis) och ligger på nätverket så ransomware kan kryptera den. Personal inte tränad på phishing. Kund- och personaluppgifter ligger i samma databas vilket ökar risken om databasen kompromitteras. Uppfyller inte NIS2 eller GDPR Artikel 32 krav.

Ytterligare skydd som behövs

1. **Bättre backup:** Daglig backup istället för veckovis. Minst en backup offline (inte kopplad till nätverk). Testa återställning varje kvartal. Referens: MSBFS Kap 3 § 36-37.
2. **Förbättrad e-postsäkerhet:** Bättre filter för phishing och skadliga bilagor. Blockera riskfyllda filtyper. Referens: MSBFS Kap 3 § 29.
3. **Nätverkssegmentering:** Separera servrar från vanliga användardatorer så ransomware inte kan sprida sig lika lätt. Ha separata databaser för kund- respektive personaluppgifter för att bättre skydda och isolera dem. Referens: MSBFS Kap 3 § 11.
4. **Utbildning:** Träna personal på att känna igen phishing-mail. Genomför test-mail regelbundet, finns automatiserade lösningar. Referens: MSBFS Kap 2 § 11.