2026-02-23

Utförd av: Julian Rieger julian.rieger@greentyre.se

Hos: GreenTyre Recycling AB

Sammanfattning

Denna risk- och sårbarhetsanalys (RSA) genomfördes för GreenTyre Recycling AB (~85 anställda), klassad som viktig entitet under NIS2-direktivet (EU 2022/2555). Analysens fokus är Identity and Access Management (IAM) i företagets hybridmiljö med lokalt Active Directory DS (greentyre.local) och Microsoft Entra ID (M365 Business Premium). Sju riskområden har identifierats och bedömts.

Risk 1 – Inloggning: Svaga autentiseringsmekanismer och avsaknad av MFA ökar risken för obehörig åtkomst. Risknivå: Hög (Röd).
Risk 2 – SSO: Kompromitterad SSO-federation kan ge angripare tillgång till alla anslutna tjänster utan ytterligare autentisering. Risknivå: Medel (Gul).
Risk 3 – Users och Segregation of Duty: Bristande rollseparation och felaktiga behörigheter möjliggör insiderhot och oavsiktliga fel. Risknivå: Medel (Orange).
Risk 4 – PIM och PAM: Permanent privilegierad åtkomst utan kontroll skapar kritisk exponering vid kompromitterade administratörskonton. Risknivå: Hög (Röd).
Risk 5 – Ransomware: Ransomware-angrepp kan kryptera verksamhetskritisk data och lamslå produktionen. Åtgärd: strukturerad backupstrategi (daglig, veckovis, månadsvis, halvårsvis) samt testad återställningsplan. Risknivå: Hög (Röd).
Risk 6 – Phishing och säkerhetsmedvetenhet: Bristande utbildning och avsaknad av trygg rapporteringskultur gör personal till den svagaste länken. Risknivå: Hög (Röd).
Risk 7 – Leverantörskedja och extern åtkomst: Externa konsulter och programvarutjänster hanteras utan formella säkerhetskrav, i strid med NIS2 Art. 21.2(d). Risknivå: Medel–Hög (Orange).

Dokumentation av hot – Risk 1

Benämning

Svaga autentiseringsmekanismer vid inloggning

Referens till ISO/IEC 27002:2022

5.17 – Autentiseringsinformation
8.5 – Säker autentisering
8.3 – Informationsåtkomstbegränsning

Analysen har genomförts med hjälp av: IT-säkerhetskonsult Julian Rieger, IT-chef, Systemadministratör AD/Entra ID

Beskrivning

Bakgrund (område, inblandad teknik/utrustning, påverkad personal, ägare, scenario)

GreenTyre Recycling AB har en hybridmiljö med lokalt Active Directory DS (greentyre.local) och Microsoft Entra ID. Inloggning till interna system sker via AD DS-konton och till M365-tjänster via Entra ID. Risken avser svaga lösenordspolicyer, avsaknad av multifaktorautentisering (MFA) på alla konton samt bristande övervakning av inloggningsförsök. Berör all personal (~85 anställda). Systemägare: IT-chef.

Konsekvenser

Med avseende på verksamhet, goodwill, ekonomi

Obehörig åtkomst till interna system och M365-tjänster (e-post, SharePoint, Teams). Ryktesskada vid dataintrång. Ekonomiska sanktioner under NIS2 Art. 32 (upp till 10 MEUR eller 2 % av global omsättning). Risk för GDPR-brott vid exponering av personaluppgifter.

Riskbedömning

Markera den bedömda risken i matrisen (K = Konsekvens, S = Sannolikhet):

K \ S	**Låg**	Mellan	**Hög**	**Väldigt hög**
Allvarlig			**X**	
Betydlig				
Måttlig				
Försumbar				

Åtgärder

Nuvarande skydd

Lösenordspolicy i AD DS (minst 8 tecken). MFA ej aktiverat på samtliga konton. Grundläggande inloggningsloggning i AD DS-händelseloggar.

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

Ytterligare skydd som behövs

Aktivera MFA på samtliga konton via Microsoft Entra ID (Authenticator-app eller FIDO2-nyckel).
Uppgradera lösenordspolicy: minst 12 tecken, komplexitetskrav, lösenordshistorik.
Inför Conditional Access-policyer (blockera inloggning från okända länder, kräv MFA vid riskfyllda inloggningar).
Aktivera Microsoft Entra ID Protection och konfigurera alert vid anomal inloggningsaktivitet.

Dokumentation av hot – Risk 2

Benämning

Kompromitterad SSO-federation ger bred obehörig åtkomst

Referens till ISO/IEC 27002:2022

5.17 – Autentiseringsinformation
8.2 – Privilegierade åtkomsträttigheter
8.3 – Informationsåtkomstbegränsning

Analysen har genomförts med hjälp av: IT-säkerhetskonsult Julian Rieger, IT-chef, Systemadministratör AD/Entra ID

Beskrivning

Bakgrund (område, inblandad teknik/utrustning, påverkad personal, ägare, scenario)

GreenTyre använder SSO (Single Sign-On) via Microsoft Entra ID, federerat mot det lokala AD DS. Om SSO-federationen kompromitteras – t.ex. via stulna tokens (token-replay), pass-the-ticket-attacker mot Kerberos eller felkonfiguration av federationsförtroende, kan en angripare få åtkomst till samtliga anslutna tjänster utan separata lösenord. Berör all personal. Systemägare: Systemadministratör AD/Entra.

Konsekvenser

Med avseende på verksamhet, goodwill, ekonomi

Bred, svårdetekterad obehörig åtkomst till samtliga M365-tjänster och interna webbapplikationer. Möjlighet att exfiltrera eller manipulera affärskritisk data. Utan sessionsövervakning kan intrånget pågå länge, vilket försvårar incidentrapportering under NIS2 Art. 23 (tidig varning 24 h, anmälan 72 h).

Riskbedömning

Markera den bedömda risken i matrisen (K = Konsekvens, S = Sannolikhet):

K \ S	Låg	Medel	Hög	Väldigt Hög
Allvarlig	X			
Betydlig				
Måttlig				
Försumbar				

Åtgärder

Nuvarande skydd

Microsoft Entra ID SSO aktiverat med grundläggande säkerhetsinställningar. Inga ytterligare token-skyddsmekanismer konfigurerade. Ingen aktiv SIEM-integration.

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

Ytterligare skydd som behövs

Aktivera Microsoft Defender for Identity för att detektera pass-the-ticket och liknande angrepp mot Kerberos.

Inför SIEM-integration (t.ex. Microsoft Sentinel) med alert vid avvikande sessionsaktivitet.

Dokumentation av hot – Risk 3

Benämning

Bristande rollseparation och felaktiga behörigheter (SoD)

Referens till ISO/IEC 27002:2022

5.3 – Ansvarsfördelning
5.18 – Åtkomsträttigheter
8.2 – Privilegierade åtkomsträttigheter

Analysen har genomförts med hjälp av: IT-säkerhetskonsult Julian Rieger, IT-chef, HR-chef

Beskrivning

Bakgrund (område, inblandad teknik/utrustning, påverkad personal, ägare, scenario)

GreenTyre saknar en konsekvent tillämpad rollbaserad åtkomstkontroll (RBAC) och Segregation of Duty (SoD). Utan tydlig rollseparation kan användare ha överlappande eller kumulativa behörigheter som möjliggör bedrägeri, oavsiktliga fel eller insiderhot. IGDLA-principen (Identities → Global Groups → Domain Local Groups → Access) tillämpas inte konsekvent i AD DS. Berör all personal med systemåtkomst. Systemägare: IT-chef.

Konsekvenser

Med avseende på verksamhet, goodwill, ekonomi

Insiderhot och bedrägeri möjliggörs när samma person kan initiera och attestera transaktioner. Risk för oavsiktlig datamanipulation. GDPR-brott vid obehörig åtkomst till personuppgifter. Svårt att spåra ansvarskedja vid incident.

Riskbedömning

Markera den bedömda risken i matrisen (K = Konsekvens, S = Sannolikhet):

K \ S	låg	Mellan	Hög	Väldigt Hög
Allvarlig				
Betydlig			X	
Måttlig				
Försumbar				

Åtgärder

Nuvarande skydd

Manuell och ad hoc-baserad behörighetshantering i AD DS. Ingen formell process för access review eller behörighetsavstämning vid rollbyten och avslutade anställningar.

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

Ytterligare skydd som behövs

Implementera IGDLA-strukturen konsekvent i AD DS för all behörighetsstyrning.
Inför halvårsvisa access reviews för att granska och rensa föråldrade behörigheter.
Definiera rollprofiler (jobbroll → behörigheter) och automatisera provisionering via koppling till HR-systemet.
Aktivera Entra ID Access Reviews för M365-grupper och applikationsåtkomst.

Dokumentation av hot – Risk 4

Benämning

Otillräcklig kontroll av privilegierade konton (PIM/PAM)

Referens till ISO/IEC 27002:2022

8.2 – Privilegierade åtkomsträttigheter
8.18 – Användning av privilegierade programverktyg
8.34 – Skydd av informationssystem under revision

Analysen har genomförts med hjälp av: IT-säkerhetskonsult Julian Rieger, IT-chef, Systemadministratör AD/Entra ID

Beskrivning

Bakgrund (område, inblandad teknik/utrustning, påverkad personal, ägare, scenario)

Domänadministratörskonton och andra privilegierade konton i GreenTyres AD DS och Entra ID har permanent tilldelade höga rättigheter utan tidsbegränsning eller krav på motivering (just-in-time. Lösenord för tjänstekonton roteras sällan. Berör IT-personal med administratörsrättigheter. Systemägare: Systemadministratör AD/Entra.

Konsekvenser

Med avseende på verksamhet, goodwill, ekonomi

Vid kompromitterat administratörskonto riskeras fullständigt systemintrång – angriparen kan nå alla system, exfiltrera data och distribuera ransomware. Utan JIT-access och PAM-loggning är skadan svår att begränsa och spåra. Kritisk NIS2-risk: långvarig störning av samhällsviktig verksamhet.

Riskbedömning

Markera den bedömda risken i matrisen (K = Konsekvens, S = Sannolikhet):

K \ S	Låg	Mellan	Hög	Väldigt hög
Allvarlig			X	
Betydlig				
Måttlig				
Försumbar				

Åtgärder

Nuvarande skydd

Separata administratörskonton finns i AD DS men utan tidsbegränsad åtkomst eller JIT-krav. Ingen MFA specifikt för privilegierade åtgärder. Lösenordsrotation för tjänstekonton sker oregelbundet.

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

Ytterligare skydd som behövs

Aktivera Entra ID Privileged Identity Management (PIM) med just-in-time-åtkomst och tidsbegränsade roller.
Kräv MFA och godkännande från IT-chef vid aktivering av privilegierade Entra ID-roller.
Implementera Microsoft LAPS (Local Administrator Password Solution) för lokala administratörslösenord på alla klientdatorer.
Rotera AD DS-tjänstekontolösenord halvårsvis; övergå till gMSA (group Managed Service Accounts).
Aktivera detaljerad revision (auditing) av privilegierade åtgärder i både AD DS och Entra ID.

Dokumentation av hot – Risk 5

Benämning

Ransomware-angrepp med kryptering av verksamhetskritisk data

Referens till ISO/IEC 27002:2022

8.13 – Säkerhetskopiering av information
8.7 – Skydd mot skadlig kod
5.30 – IKT-beredskap för verksamhetskontinuitet
8.15 – Loggning

Analysen har genomförts med hjälp av: IT-säkerhetskonsult Julian Rieger, IT-chef, Driftansvarig

Beskrivning

Bakgrund (område, inblandad teknik/utrustning, påverkad personal, ägare, scenario)

GreenTyre Recycling AB exponeras för ransomware-angrepp via vanliga angreppsvektorer: nätfiske (phishing), komprometterade inloggningsuppgifter, exponerade RDP-tjänster och sårbarheter i opatchade system. Vid ett lyckat angrepp krypteras filer på servrar och klientdatorer, vilket kan lamslå produktion och administration. Berör all personal och samtliga IT-system. Systemägare: IT-chef / Driftansvarig.

Konsekvenser

Med avseende på verksamhet, goodwill, ekonomi

Produktionsstopp och intäktsbortfall under återställningsperioden. Utpressningskrav (lösen) med risk för dataläckage om lösen ej betalas. Ryktesskada och förtroendeskada gentemot kunder och leverantörer. NIS2-krav på incidentrapportering (Art. 23): tidig varning 24 h, anmälan 72 h, slutrapport 1 månad. Risk för GDPR-sanktioner vid exponering av personuppgifter.

Riskbedömning

Markera den bedömda risken i matrisen (K = Konsekvens, S = Sannolikhet):

K \ S	**Låg**	**Mellan**	**Hög**	Väldigt hög
Allvarlig			X	
Betydlig				
Måttlig				
Försumbar				

Åtgärder

Nuvarande skydd

Grundläggande antivirusskydd på klientdatorer. Inga strukturerade, testade backuprutiner. Ingen nätverkssegmentering som begränsar spridning. Ingen EDR-lösning (Endpoint Detection and Response).

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

Ytterligare skydd som behövs

Implementera strukturerad backupstrategi med följande rotationsschema:

- Daglig säkerhetskopiering (inkrementell) – behålls 30 dagar
- Veckovis säkerhetskopiering (full) – behålls 3 månader
- Månadsvis säkerhetskopiering (full, offsite/molnlagring) – behålls 1 år
- Halvårsvis säkerhetskopiering (full, arkivering) – behålls 5 år

Lagra minst en backupkopia offline eller i isolerad molnmiljö (immutable storage, t.ex. Azure Blob Storage) så att ransomware inte kan kryptera backupen.

Upprätta och dokumentera en testad rollback- och återställningsplan: planen ska testas minst en gång per halvår med faktisk återläsning av backup till testmiljö, och testet ska protokollföras med ansvarig och datum.

Aktivera Microsoft Defender for Endpoint (EDR) på alla klientdatorer och servrar för realtidsdetektering och automatisk isolering vid misstänkt aktivitet.

Inför nätverkssegmentering för att begränsa lateral rörelse vid ett intrång (separera OT-nät, adminsnät och användarnät).

Säkerställ att alla system är patchade inom 30 dagar efter kritiska säkerhetsuppdateringar.

Dokumentation av hot – Risk 6

Benämning

Phishing och bristande säkerhetsmedvetenhet hos personal

Referens till ISO/IEC 27002:2022

6.3 – Säkerhetsmedvetenhet, utbildning och träning
6.8 – Rapportering av informationssäkerhetshändelser
8.7 – Skydd mot skadlig kod

Analysen har genomförts med hjälp av: IT-säkerhetskonsult Julian Rieger, IT-chef, HR-chef

Beskrivning

Bakgrund (område, inblandad teknik/utrustning, påverkad personal, ägare, scenario)

Den vanligaste ingångspunkten för cyberangrepp mot GreenTyre är den mänskliga faktorn. Phishing-e-post, smishing (SMS) och social ingenjörskonst riktar sig mot enskilda medarbetare för att lura dem att lämna ut inloggningsuppgifter, öppna skadliga bilagor eller klicka på manipulerade länkar. Utan regelbunden utbildning och en trygg rapporteringskultur riskerar incidenter att döljas eller att uppföljas för sent. Berör all personal (~85 anställda). Systemägare: IT-chef / HR-chef.

Konsekvenser

Med avseende på verksamhet, goodwill, ekonomi

Lyckade phishing-attacker leder till kompromitterade konton, spridning av skadlig kod (inkl. ransomware) och dataläckage. Om medarbetare är rädda för att rapportera misstag fördröjs IT:s förmåga att begränsa skadan, vilket försvårar efterlevnad av NIS2:s incidentrapporteringskrav (Art. 23). Ryktesskada och GDPR-sanktioner vid exponering av personuppgifter.

Riskbedömning

Markera den bedömda risken i matrisen (K = Konsekvens, S = Sannolikhet):

K \ S	**Låg**	**Mellan**	Hög	**Väldigt Hög**
Allvarlig				
Betydlig				**X**
Måttlig				
Försumbar				

Åtgärder

Nuvarande skydd

Ingen strukturerad säkerhetsutbildning för personal. Ingen formell process för rapportering av misstänkta e-postmeddelanden eller incidenter. Grundläggande skräppostfilter i M365.

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

Ytterligare skydd som behövs

Inför obligatorisk, årlig säkerhetsmedvetenhetsutbildning för all personal – med fokus på att känna igen phishing, social ingenjörskonst och misstänkta bilagor/länkar.
Genomför regelbundna simulerade phishing-övningar (t.ex. via Microsoft Attack Simulator) för att mäta och förbättra personalens kritiska tänkande.
Etablera en öppen rapporteringskultur: det ska aldrig vara pinsamt att kontakta IT om man råkat klicka på något misstänkt eller kört ett program som kändes fel – tidig rapportering begränsar alltid skadan.
Skapa en enkel rapporteringskanal (t.ex. dedikerad e-postadress eller "Rapportera phishing"-knapp i Outlook) så att tröskeln att höra av sig är låg.
Bekräfta och tacka personal som rapporterar – positiv förstärkning av rätt beteende är mer effektivt än sanktioner vid misstag.
Dokumentera alla rapporterade incidenter och misstänkta händelser i en logg som IT granskar veckovis.

Dokumentation av hot – Risk 7

Benämning

Bristande säkerhetskrav i leverantörskedjan – externa konsulter och programvarutjänster

Referens till ISO/IEC 27002:2022

5.19 – Informationssäkerhet i leverantörsrelationer
5.20 – Hantering av informationssäkerhet inom leverantörsavtal
5.21 – Hantering av informationssäkerhet i IKT-leveranskedjan
5.22 – Uppföljning, granskning och förändringsstyrning av leverantörstjänster

Analysen har genomförts med hjälp av: IT-säkerhetskonsult Julian Rieger, IT-chef, Inköpsansvarig/Juridik

Beskrivning

Bakgrund (område, inblandad teknik/utrustning, påverkad personal, ägare, scenario)

GreenTyre Recycling AB anlitar externa IT-konsulter och nyttjar ett antal externa programvarutjänster (SaaS/molntjänster). Externa konsulter ges åtkomst till interna system utan standardiserad IAM-process: det saknas rutin för tidsbegränsade konton, MFA-krav, åtkomstnivåprincip (minsta privilegium) och avprovisionering vid uppdragets slut. Externa programvarutjänster integreras mot AD DS/Entra ID utan formell säkerhetsgranskning. Enligt NIS2 Art. 21.2(d) och Art. 21.3 är GreenTyre skyldigt att ställa motsvarande säkerhetskrav på sina leverantörer och tjänsteleverantörer. Berör IT-avdelning, inköp och ledning. Systemägare: IT-chef / Inköpsansvarig.

Konsekvenser

Med avseende på verksamhet, goodwill, ekonomi

En kompromitterad extern konsult eller en sårbar SaaS-tjänst kan ge angripare direkt åtkomst till GreenTyres interna miljö – utan att passera den egna perimeterskyddet. Glömda konsultkonton utgör permanenta bakdörrar. Bristande leverantörskrav strider mot NIS2 Art. 21.2(d) och kan leda till administrativa sanktioner (upp till 10 MEUR, Art. 32). Tredjepartsintrång kan utlösa NIS2-incidentrapportering och GDPR-anmälan.

Riskbedömning

Markera den bedömda risken i matrisen (K = Konsekvens, S = Sannolikhet):

K \ S	**Låg**	**Mellan**	**Hög**	**Väldigt hög**
Allvarlig		X		
Betydlig				
Måttlig				
Försumbar				

Åtgärder

Nuvarande skydd

Externa konsulter tilldelas konton ad hoc utan formell process. Inga kontraktuella säkerhetskrav ställs på leverantörer. Ingen inventering av externa programvarutjänster (SaaS-register saknas). Ingen rutin för avprovisionering vid uppdragets slut.

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

Ytterligare skydd som behövs

Inför en formell IAM-process för externa konsulter: tidsbegränsade konton (max uppdragsperiod), MFA-krav, minsta-privilegium-åtkomst och automatisk avprovisionering vid uppdragets slut.

Upprätta ett register (SaaS-inventering) över alla externa programvarutjänster med koppling till AD DS/Entra ID – granska och godkänn varje integration säkerhetsmässigt innan driftsättning.

Inför kontraktuella säkerhetskrav (NIS2-klausul) i alla leverantörsavtal: leverantören ska uppfylla motsvarande säkerhetsnivå som GreenTyre, kunna uppvisa certifiering (t.ex. ISO 27001) eller genomgå säkerhetsgranskning.

Genomför årliga leverantörsutvärderingar där säkerhetsefterlevnad granskas – dokumentera resultat och kräv åtgärdsplan vid avvikelser.

Kräv att externa konsulter använder egna MFA-skyddade konton (gäst-/B2B-konton via Entra ID External Identities) snarare än delade eller interna konton.

Säkerställ att alla externa tjänster loggar åtkomst och att loggarna är tillgängliga för GreenTyre vid incidentutredning.

GAP-analys

Tabellen nedan jämför GreenTyre Recycling ABs nuvarande läge (AS-IS) mot de krav som ställs av NIS2-direktivet (Art. 21) och ISO/IEC 27002:2022 inom varje identifierat riskområde. Prioritet bedöms utifrån risknivå och åtgärdens effekt på säkerhetsnivån.

Område	Krav (NIS2 / ISO 27002:2022)	Nuläge (AS-IS)	GAP / Brist	Prioritet
Inloggning (Risk 1)	MFA på alla konton, stark lösenordspolicy (≥12 tecken), Conditional Access, inloggningsövervakning (NIS2 Art. 21; ISO 8.5, 5.17)	Lösenordspolicy 8 tecken. MFA ej aktiverat på alla konton. Begränsad loggning. Ingen Conditional Access.	MFA saknas på majoriteten av konton. Lösenordspolicy för svag. Conditional Access och Entra ID Protection inte konfigurerade.	**Hög**
SSO (Risk 2)	Token-skydd (, kort livstid), sessionsövervakning, SIEM-integration, Defender for Identity (NIS2 Art. 21; ISO 5.17, 8.3)	Entra ID SSO aktiverat med standardinställningar. Ingen SIEM eller token-skyddsmekanismer konfigurerade.	Defender for Identity inte aktiverat. Ingen SIEM-integration.	**Medel**
Users & SoD (Risk 3)	RBAC med IGDLA, formell SoD-policy, regelbundna access reviews, automatiserad provisionering (NIS2 Art. 21; ISO 5.3, 5.18)	Manuell behörighetshantering i AD DS. Ingen formell SoD-policy. Inga access reviews eller rollprofiler.	IGDLA ej implementerat konsekvent. Inga halvårsvisa access reviews. Ingen koppling HR-system → behörighetsprovisionering.	**Medel**
PIM/PAM (Risk 4)	JIT-åtkomst (PIM), MFA för privilegierade åtgärderprivilegierad auditing (NIS2 Art. 21; ISO 8.2, 8.18)	Permanenta adminrättigheter utan tidsbegränsning. Ingen PAM/PIM. LAPS ej implementerat. Oregelbunden lösenordsrotation.	Entra ID PIM inte aktiverats. Ingen auditing av privilegierade åtgärder i AD DS eller Entra ID.	**Hög**
Ransomware (Risk 5)	Strukturerad backupstrategi (daglig/veckovis/månadsvis/halvårsvis), immutable offsite-backup, dokumenterad och testad återställningsplan, EDR (NIS2 Art. 21; ISO 8.13, 8.7, 5.30)	Grundläggande antivirus. Inga strukturerade backuprutiner. Ingen EDR eller nätverkssegmentering. Ingen testad återställningsplan.	Backupstrategi (daglig/veckovis/månadsvis/halvårsvis) saknas. Ingen immutable backup. Återställningsplan finns ej dokumenterad eller testad.	**Hög**
Phishing & Säkerhets-medvetenhet (Risk 6)	Obligatorisk säkerhetsutbildning, phishing-simuleringar, trygg rapporteringskultur, enkel rapporteringskanal (NIS2 Art. 21; ISO 6.3, 6.8)	Ingen strukturerad säkerhetsutbildning. Ingen formell rapporteringsprocess. Grundläggande skräppostfilter i M365.	Utbildning saknas helt. Ingen phishing-simulering. Rapporteringskultur ej etablerad – medarbetare kan vara rädda att rapportera misstag.	**Hög**
Leverantörs-kedja & Extern åtkomst (Risk 7)	IAM-process för externa konsulter (tidsbegr. konton, MFA, avprovisionering), SaaS-inventering, NIS2-klausul i avtal, årlig leverantörsgranskning (NIS2 Art. 21.2(d); ISO 5.19–5.22)	Konsultkonton skapas ad hoc utan rutin. Inga kontraktuella säkerhetskrav. Inget SaaS-register. Ingen avprovisioneringspro	Ingen IAM-process för externa konton. NIS2-klausul saknas i leverantörsavtal. SaaS-tjänster ej granskade. Leverantörsutvärdering saknas.	**Hög**

		cess.		

Samtliga GAP kräver åtgärd. Högt prioriterade GAP (Inloggning, PIM/PAM, Ransomware, Phishing/Säkerhetsmedvetenhet och Leverantörskedja) bör åtgärdas omgående för att uppfylla NIS2:s krav på lämpliga och proportionella säkerhetsåtgärder (Art. 21.1) samt leverantörskraven i Art. 21.2(d).