

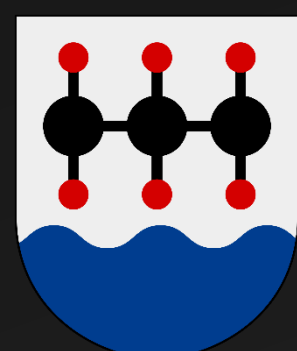
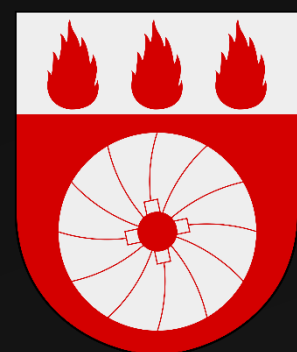
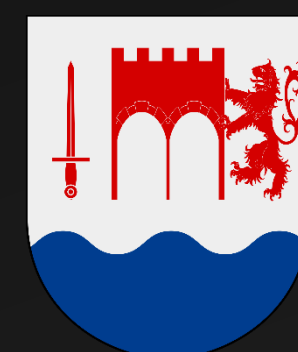
DB24^{LIVE} **KommITS**

*När ni har ett intrång –
Vad önskar du då att du redan
gjort?_*

Så skyddar du din dataplattform innan det är för sent



Ett urval av de kommuner som vi arbetar med idag



*När du har ett intrång – vad
önskar du att du redan gjort?_*

*”Går systemet ner är det en
fråga om rikets säkerhet”_*

MSB har tydligt metodstöd och konsekvenserna när data läcker är allvarliga.

Konsekvensnivåer				
Värdering	Invånare/medarbetare	Avbrott i verksamheten	Ekonomisk skada	Minskat förtroende
4. Allvarlig	Allvarlig påverkan för medarbete, invånare eller brukare. Individens liv och hälsa kan äventyras.	Allvarlig påverkan på verksamhetens förmåga, omöjligt eller nästan omöjligt att fullfölja uppdragen.	Mycket stor ekonomisk skada. 2 miljoner kronor och uppåt eller avvikelse på 15% av budget.	Förtroendet för kommunen är negativt påverkat i allvarlig grad. Ihållande drev i rikstäckande medier eller av organiserade grupperingar i sociala medier.
3. Betydande	Större påverkan för medarbete, invånare eller brukare. Enskilda individer kan uppleva konsekvenser, såsom stora besvär.	Verksamheten kan fullfölja sina uppdrag men med trolig risk för kännbar påverkan exempelvis genom att behöva vidta extraordinära åtgärder.	Stor ekonomisk skada. 500 000 – 2 miljoner kronor eller avvikelse på 10–15% av budget.	Förtroendet för kommunen är negativt påverkat i hög grad. Nyheter i både riks- och lokalmedia men begränsat till enskilda händelser eller enskilda individers agerande.
2. Måttlig	Viss påverkan för medarbete, invånare eller brukare. Enskilda individer kan notera störningen eller uppleva lindriga besvär.	Viss påverkan på verksamhetens förmåga, inga större svårigheter att fullfölja uppdragen.	Viss ekonomisk skada. 1 – 500 000 kronor eller avvikelse på 5–10% av budget.	Förtroendet för kommunen är negativt påverkat till liten grad. Enstaka missnöjda individer uttalar sig i sociala medier eller lokalmedia.
1. Försumbar	Ingen eller försumbar påverkan för medarbete, invånare eller brukare.	Ochotvillig påverkan på verksamhetens förmåga, inga större svårigheter att fullfölja uppdragen.	Ingen märkbar ekonomisk skada.	Liten negativ uppmärksamhet.

Sannolikhetsnivåer

Värdering

Beskrivning/kriterier

4. Sannolik

Har inträffat förr, förväntas hända inom 12 månader.

3. Möjlig

Finns flera kända fall, förväntas hända inom fem år.

2. Mindre sannolik

Finns kända fall, kan hända inom fem år.

1. Osannolik

Har aldrig hänt förr, förväntas inte hända inom överskådlig framtid.

Summerring: Vad står på spel? _

Kort om mig _

Andreas Evander

Partner/Founder DB24

DB24 CEO & Stategic Lead

Data- & säkerhetsnörd med förkärlek för verkliga problem

Föreläsare, rådgivare & orädd SQL-evangelist

Tidigare drifttekniker som fortfarande gillar att skruva på saker

SQL User Group Board Member

50+ Kommuner kör DB24 programvaran

En nörd i kostym – som hjälper Sveriges kommuner att sova lite tryggare om nätterna.

(Fortfarande med drömmen om att äga en grävmaskin.)



*Hur kan detta hända? _
Vi saknar data över vårt data...*

- Har vi audit på dataplattformen,
- Nej vi kan ta fram info om någon vill ha den

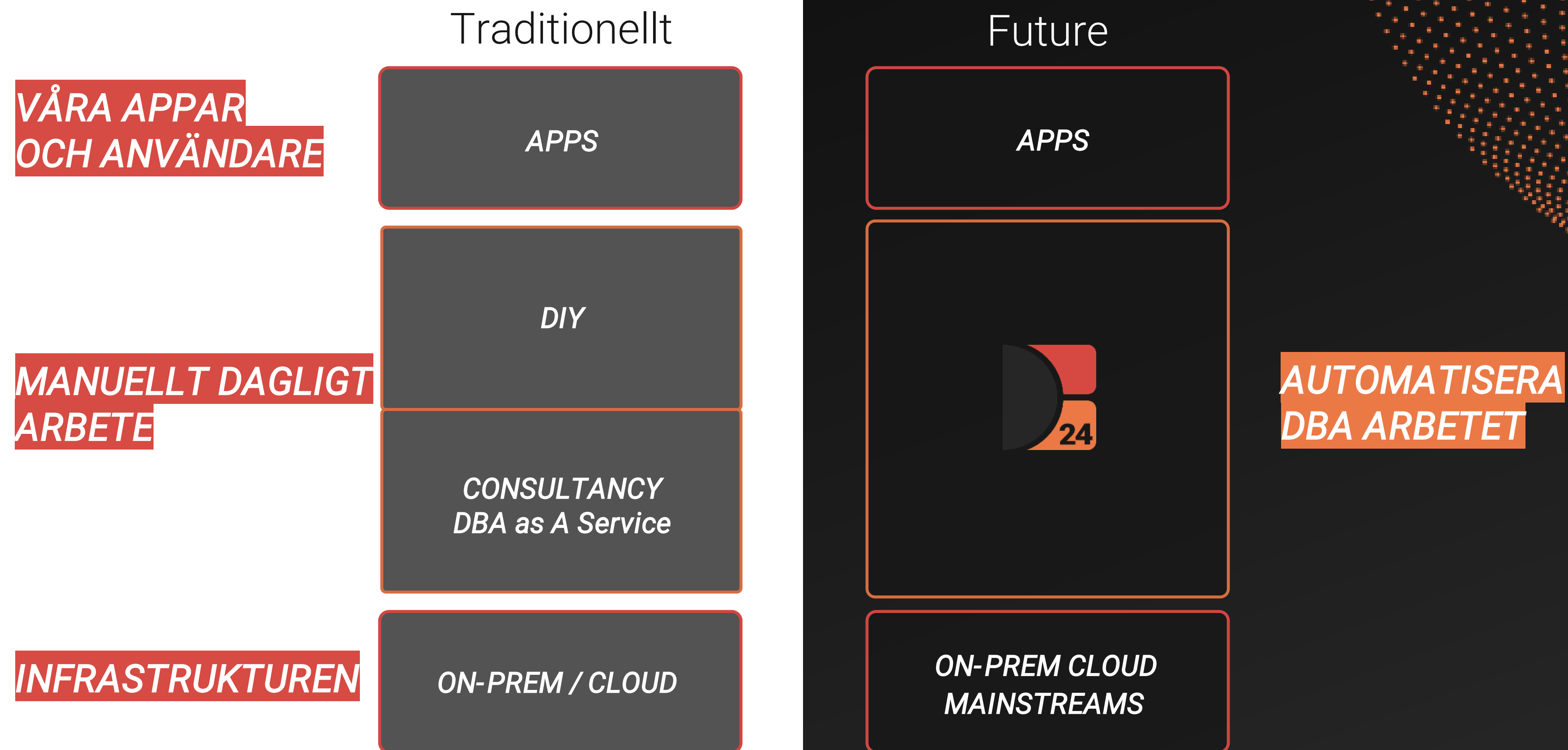
- Har vi antivirus
- Nej vi kan installera strax innan någon tänker attackera oss

0% av de 354 organisationer som DB24 träffade under 2024 hade ett CMDB över sin mest värdefulla asset, sin data.

0% hade spårning av förändringar i dataplattformen



Traditionella lösningar fungerar inte längre



*Det är databasen som är Er
akilleshäl! _*

När en dataläcka inträffar, vad är det som går fel? _

Här är Era system en guldgruva pga höga behörigheter i många led

Här är dataplattformarna utsatta, det saknas nästan alltid lösenordspolicies för SQL konton ”sommar1” är absolut gångbart lösenord

Här börjar det blir väldigt enkelt, ofta eftersatt livscyklng, ofta dåligt säkrade test system.

Nu är det som att stjäla godis ifrån barn, oskyddat och okrypterat. Sannolikt hittas en backup som ligger och skräpar så coola data extraction script behövs inte ens

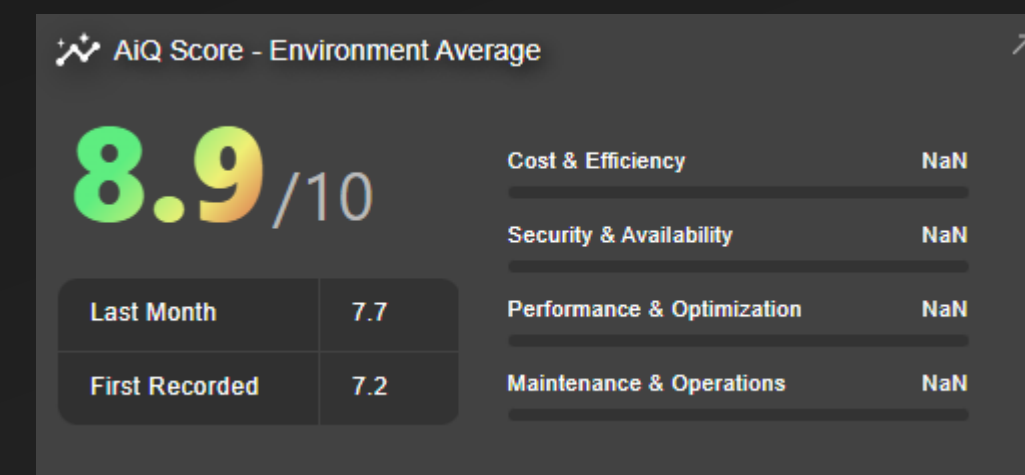
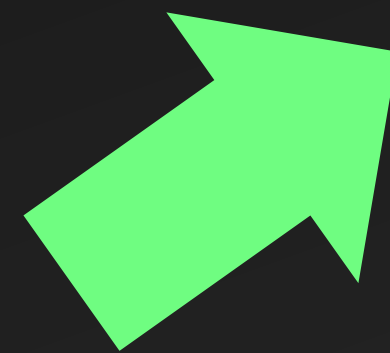
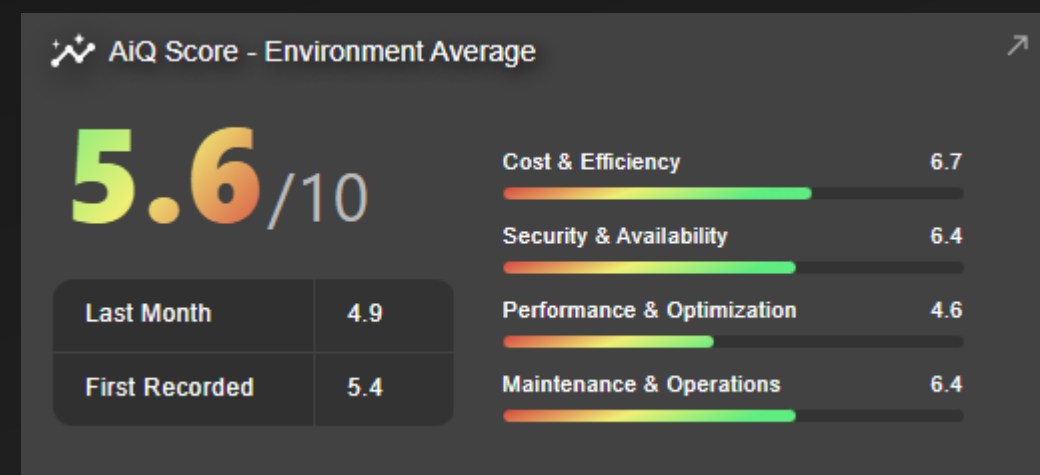
Sista steget är att via TOR network ladda upp databasbackuper, ingen audit fanns på plats så ingen kommer dessutom upptäcka vad som gjorts.

ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance 11 techniques	Resource Development 8 techniques	Initial Access 11 techniques	Execution 17 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 47 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (13)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Archive Collected Data (3)	Communication Through Removable Media	Content Injection	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Audio Capture	Automated Collection	Dynamic Resolution (3)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Browser Session Hijacking	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Exploitation for Client Execution	Compromise Host Software Binary	Boot or Logon Initialization Scripts (5)	Delay Execution	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Cloud Storage	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Input Injection	Create Account (3)	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Email Bombing
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Inter-Process Communication (3)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Deploy Container	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Information Repositories (6)	Fallback Channels	Scheduled Transfer	Endpoint Denial of Service (4)
Search Open Websites/Domains (3)		Trusted Relationship	Native API	Event Triggered Execution (18)	Escape to Host	Direct Volume Access	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Local System	Hide Infrastructure	Transfer Data to Cloud Account	Financial Theft
Search Threat Vendor Data		Valid Accounts (4)	Poisoned Pipeline Execution	Exclusive Control	Event Triggered Execution (18)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Network Shared Drive	Ingress Tool Transfer		Firmware Corruption
Search Victim-Owned Websites		Wi-Fi Networks	Scheduled Task/Job (5)	External Remote Services	Exploitation for Privilege Escalation	Email Spoofing	Network Sniffing	Domain Trust Discovery		Data from Removable Media	Multi-Stage Channels		Inhibit System Recovery
			Serverless Execution	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Execution Guardrails (2)	OS Credential Dumping (8)	File and Directory Discovery		Data Staged (2)	Non-Application Layer Protocol		Network Denial of Service (2)
			Shared Modules	Implant Internal Image	Process Injection (12)	Exploitation for Defense Evasion	Steal Application Access Token	Group Policy Discovery		Email Collection (3)	Non-Standard Port		Resource Hijacking (4)
			Software Deployment Tools	Modify Authentication Process (9)	Scheduled Task/Job (5)	Hide Artifacts (14)	Steal or Forge Authentication Certificates	Local Storage Discovery		Input Capture (4)	Protocol Tunneling		Service Stop
			System Services (3)	Modify Registry	Valid Accounts (4)	Hijack Execution Flow (12)	Steal or Forge Kerberos Tickets (5)	Log Enumeration		Screen Capture	Proxy (4)		System Shutdown/Reboot
			User Execution (5)	Office Application Startup (6)		Impair Defenses (12)		Network Service Discovery		Video Capture	Remote Access Tools (3)		
			Windows Management Instrumentation	Power Settings				Network Sniffing			Traffic Signaling (2)		
								Password Policy Discovery			Web Service (3)		

*Summerring, varför är
våra dataplattformar
så utsatta och
eftersatta _*



~~*När du har ett intrång...*~~
~~*= vad önskar du att du redan gjort? _*~~

*- Vad skall vi hem och göra direkt för
att minimera påverkan av ett intrång*

En plan att införa i sju steg _

1. Börja med inventering, skapa ett databas över era databaser.

En plan att införa i sju steg _

- 2. Delegera ut ägarskap över system och databaser, både tekniskt och verksamhetsmässigt.*

En plan att införa i sju steg _

- 3. När inventeringen är klar, se över livscykelhantering så att allt är patchat och up-to-date*

En plan att införa i sju steg _

4. Se över konfiguration och åtgärda felaktigheter

En plan att införa i sju steg _

5. Ifrågasätt alla högre behörigheter kring er dataplattform

En plan att införa i sju steg _

6. Implementera en standardiserat databasunderhåll

En plan att införa i sju steg _

- 7. Sist och störst insats, Inför kryptering på bred front, både av data i vila samt data i transit.*

Summaring –

1. *Börja med inventering, skapa ett databas över ert data.*
2. *Delegera ut ägarskap över system och databaser, både tekniskt och verksamhetsmässigt.*
3. *När inventeringen är klar, se över livscykelhantering så att allt är patchat och up-to-date.*
4. *Se över konfiguration och åtgärda felaktigheter*
5. *Ifrågasätt alla högre behörigheter kring er dataplattform*
6. *Implementera en standardiserat databasunderhåll*
7. *Inför kryptering på bred front, både av data i vila samt data i transit.*

Det är inte Rocketscience!_

Punkt 1-6 kan man införa på minde än 4 veckor

Några exempel på kommuner och förbund som gjort det i närtid, och som gör det väldigt bra!

Punkt 7 – Kryptering är betydligt mer komplicerat men även väldigt viktigt, Soltak AB på västkusten är med sina ägarkommuner väldigt långt framme och är en förebild för hur kommunal dataplattformsdrift skall göras.

Frågor att ställa till Era organisationer:

Har vi koll på vår (näst)viktigaste tillgång, vårt data _

Vad har vi för data?

Vem ändrar?

Vem ansluter

Vilka risker finns

Vem äger riskerna



Avslutningsvis frågestund _



Jag connectar gärna på LinkedIn!

<https://www.linkedin.com/in/andreas-evander-db24/>



Soltak Modernizing Municipal IT Solutions Together with DB24_

100%

Uptime since 2019

Through DB24, Soltak AB met higher demands of availability, assuring uninterrupted service and heightened efficiency.

“
Soltak AB has used DB24 for a couple of years now and the service has truly exceeded the value we were hoping for and has evolved even more.

*Daniel Bjurström,
CIO at Soltak AB*



Filipstad Municipality Amplifies Efficiency and Reduces Costs with DB24_

//
I absolutely recommend using DB24. It's not just the cost-savings; it's the performance, reliability, and user satisfaction that now lets me sleep a bit better at night.

*Roger Nordqvist
Technical Operations Manager
IT unit, Filipstad Municipality*

 WATCH CASE STUDIE

80%
Reduction in Servers

Server consolidation reduced the database server count from 20 to just 4, enhancing resource utilization.



Shibuya Optimizes their SQL Server Environments with DB24_

//

I would recommend all companies that are using MS SQL Server for their Business-Critical Applications to look at what DB24 have to offer.

*Stefan Lindström,
Key Account Manager at Shibuya*

Time to complete workload
reduced by more than

50%