



# ZERO TRUST

SOLDIER





# ALLE HENDELSER KUNNE VÆRT UNNGÅTT. VI MÅ SLUTTE Å SI NOE ANNET!

Det er enkelt å være etterpåklok, men kanskje det er noe i det.  
La oss fokusere på det enkle og effektive.







# Mål

Misbruk av nulldagssårbarheter er ikke synonymt med å være sjakk matt.

# ← NSMs Grunnprinsipper for IKT-sikkerhet →

## Før

solarwinds



ivanti



Exchange

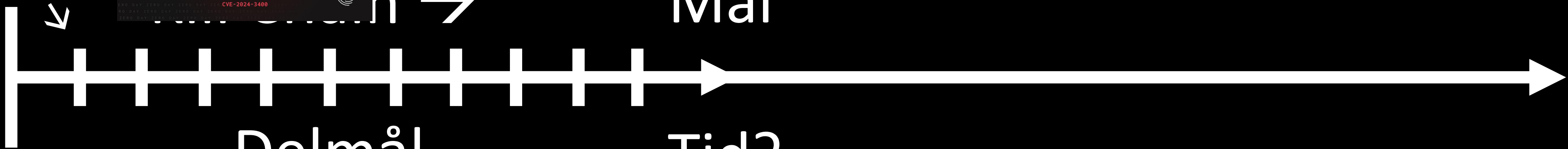


## Etter

Hele Norge øver

Nulldagssårbarhet? →

Start



Delmål

Tid?

Mål

Misbruk av nulldagssårbarheter er ikke synonymt med å være sjakk matt.

GÖRAN TÖMTE



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Escape to Host	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Modify Authentication Process (4)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion	OS Credential Dumping (8)	Group Policy Discovery		Data from Local System	Non-Application Layer Protocol	Scheduled Transfer	Resource Hijacking
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)	Steal Application Access Token	Network Service Scanning		Data from Network Shared Drive	Non-Standard Port	Transfer Data to Cloud Account	Service Stop
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (6)	Hide Artifacts (9)	Steal or Forge Kerberos Tickets (4)	Network Share Discovery		Data from Removable Media	Protocol Tunneling		System Shutdown/Reboot
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)	Steal Web Session Cookie	Network Sniffing		Data Staged (2)	Proxy (4)		
				Office Application Startup (6)		Hijack Execution Flow (11)	Two-Factor Authentication Interception	Password Policy Discovery		Email Collection (3)	Remote Access Software		
				Pre-OS Boot (5)		Impair Defenses (9)	Unsecured Credentials (7)	Peripheral Device Discovery		Input Capture (4)	Traffic Signaling (1)		
				Scheduled Task/Job (6)		Indicator Removal on Host (6)		Permission Groups Discovery (3)		Screen Capture	Web Service (3)		
				Server Software Component (4)		Indirect Command Execution		Process Discovery		Video Capture			
				Traffic Signaling (1)		Masquerading (7)		Query Registry					
				Valid Accounts (4)		Modify Authentication Process (4)		Remote System Discovery					
						Modify Cloud Compute Infrastructure (4)		Software Discovery (1)					
						Modify Registry		System Information Discovery					
						Modify System Image (2)		System Location Discovery (1)					
						Network Boundary Bridging (1)		System Network Configuration Discovery (1)					
						Obfuscated Files or Information (6)		System Network Connections Discovery					
						Pre-OS Boot (5)		System Owner/User Discovery					
						Process Injection (11)		System Service Discovery					
						Reflective Code Loading		System Time Discovery					
						Rogue Domain Controller		Virtualization/Sandbox Evasion (3)					
						Rootkit							
						Signed Binary Proxy Execution (13)							
						Signed Script Proxy Execution (1)							
						Subvert Trust Controls (6)							
						Template Injection							
						Traffic Signaling (1)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							







EUROPEAN UNION AGENCY  
FOR CYBERSECURITY



# 1. Assume vulnerable

Before

# 2. Assume breach

During

# 3. Assume ransomware

After



1. Assume vulnerable

2. Assume breach

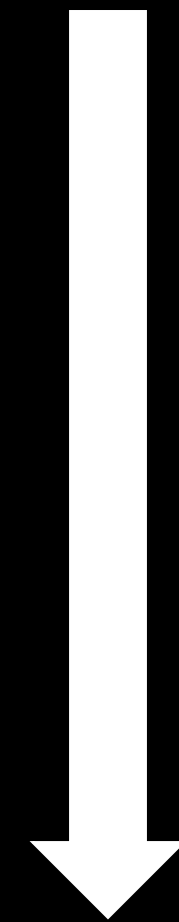
3. Assume ransomware

# On-prem

# Cloud

# Leverandører

# Least Privilege

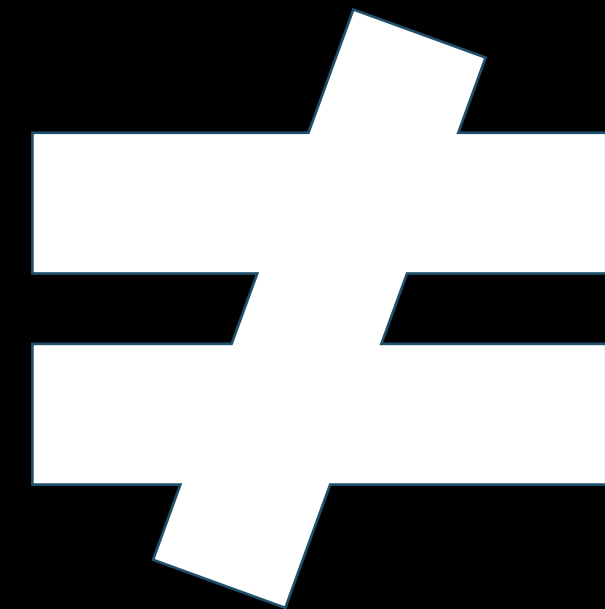


Suksessfulle hendelser skjer i tillatt trafikk.  
De beste hendelsene er de som ikke skjer.

Ledelse, mellomledelse, systemansvarlige



**ZERO DAY  
EXPLOIT**



Misbruk av nulldagssårbarheter er ikke synonymt med å være sjakk matt.

GÖRAN TÖMTE





TAKK FOR MEG



LinkedIn

GÖRAN TÖMTE