

Informations & produktions säkerhet i vindkraften

Digitaliserade och fysiska hot

Per Olofsson - 2021-11-01



W3 ENERGY

Vem är jag?

Per Olofsson



- 20 års erfarenhet från IT branschen med 14 år i Energibranschen
- Teknikintresse sedan 286:ans tid
- Äger idag W3 Energy - Den största oberoende förvaltaren av vindkraft
- Medlem i Svensk Vindkrafts styrelse sedan 2021
- Kuriosa: Är en aktiv skogsägare

W3 Energy

Active Asset Management



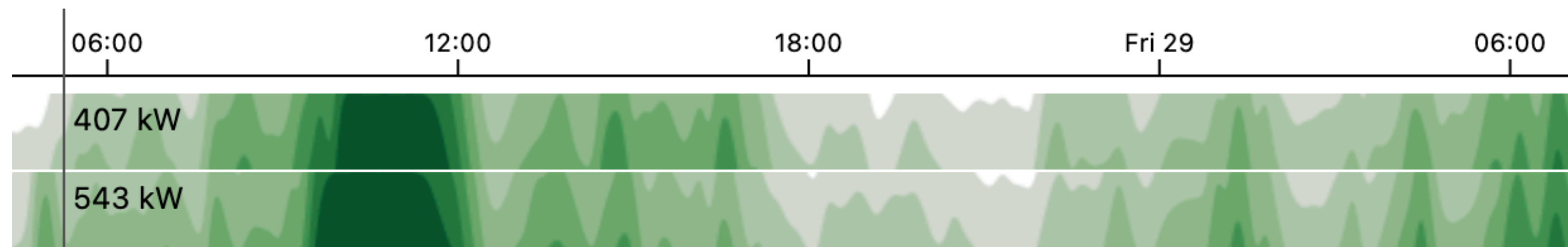
- Företagsidé: Sveriges bästa oberoende förvaltning av vindkraft
- Fördelat på två huvudområden - FMA & TMA
 - Financial Management Agreement - Redovisning, finans, beslutsstöd, bank, revision m.m.
 - Technical Management Agreement - 24/7 drift, site närvaro, vägar, elnät, fiber m.m.
- Grid - Elnät & nätstationer, Elanläggningsansvar, Eldriftsansvar
- IT - Design & Drift
- **One Stop Shop - För vindkraft & tillhörande anläggningar**

Utmaningar ur ett förvaltningsperspektiv



Investerat i en tillgång

- Ägare vill ha resultat på sista raden
- Definition: Produktionsanläggning



- Tänk om, se det som ett företag istället - med flertalet verksamhetsgrenar
- Ägare & förvaltning måste fatta väl avvägda beslut under resans gång
- Här kommer W3 Energy in i bilden

Utmaningar ur ett förvaltningsperspektiv



W3 Energy

- Vi jobbar för att du som kund ska få de bästa underlagen till beslut
- Beslut som rör verksamheten på lång sikt
- Vi jobbar proaktivt för att öka de värden som finns
- Hur kopplar detta mot informationssäkerhet?



Utmaningar ur ett förvaltningsperspektiv



Informations & produktionssäkerhet

- God koll - likaså behövs ett risk & möjlighetstänkande
- Vilka avvikelser kan ske? Vilka möjligheter uppstår?
- Allt som slutar i försämrat resultat ska vi så långt det är rimligt motverka
- “Produktionsläckage” kontra informationsläckage

- Vad måste vi göra?

Utmaningar ur ett förvaltningsperspektiv

EU har inrättat lagstiftning på området

- NIS direktivet (2018)
- Inom EU en varierande implementation av direktiven - Sverige är på god väg
- Sanktioner vid saknad lagefterlevnad
- Inrättande av *The European Cybersecurity Competence Centre and Network & Joint Cyber Unit*
- Kommande NIS 2.0 - presenterat dec 2020 - förhandlingar pågår
- —> **Hårdare sanktioner** —> **Fler branscher**

Utmaningar ur ett förvaltningsperspektiv

Lagstiftning i Sverige

- Säkerhetsskyddslag (2018:585 tom SFS 2021:76)
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- MSBFS 2018:7 (Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster)
- STEMFS 2021:3 (Statens energimyndighets föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn)

Utmaningar ur ett förvaltningsperspektiv



Lågstanivån

- NIS direktivet och senare NIS 2
- Innebär att bedriva ett systematiskt informationssäkerhetsarbete
- Börja litet och skala upp
- Gör det innan drift av vindpark AB och nätstation AB drar igång

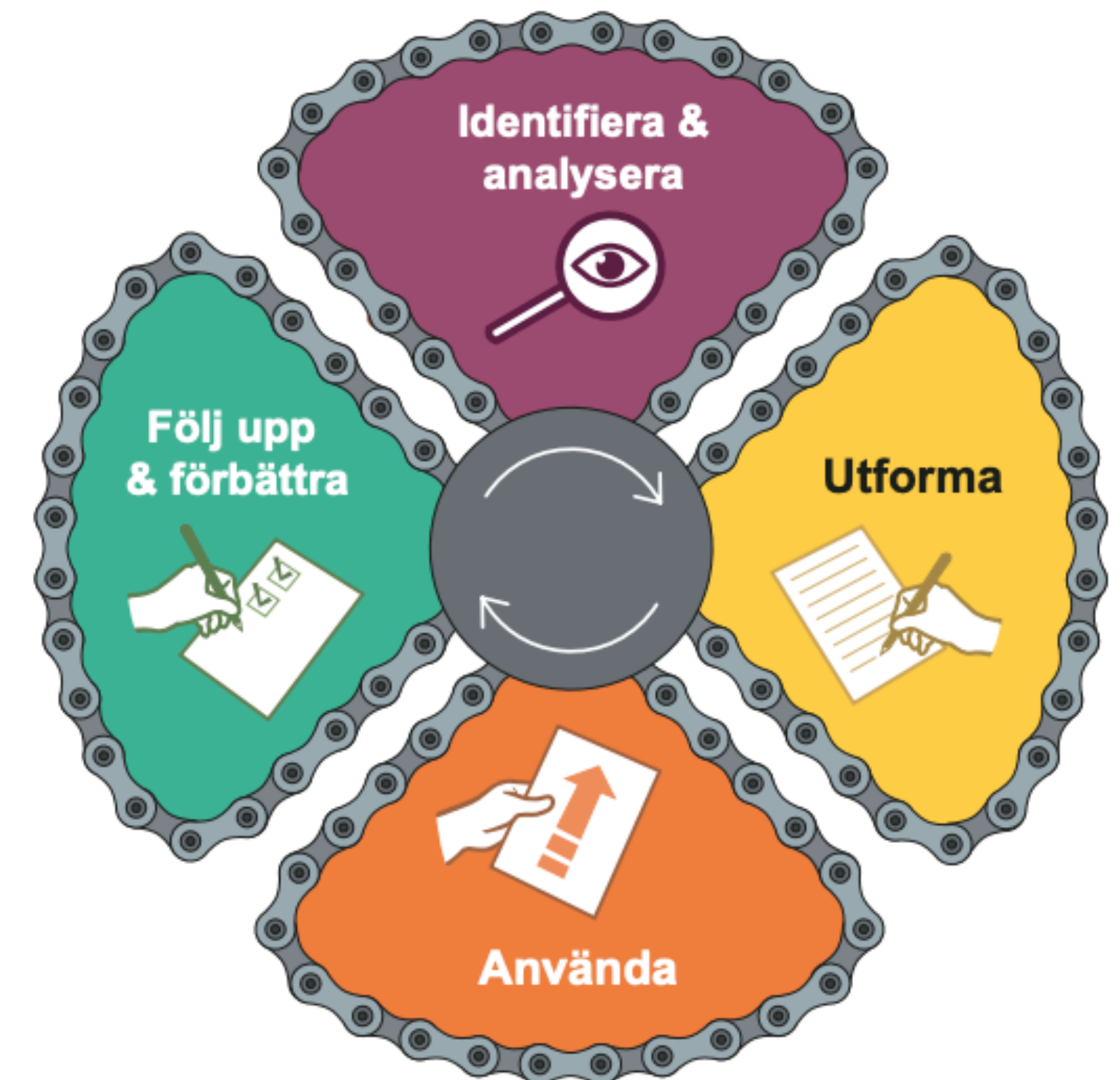


Se till att få med leverantörer i det systematiska tänket!

Utmaningar ur ett förvaltningsperspektiv

MSBs metodstöd - Några exempel

- Identifiera - utforma - använda - förbättra
- Vad gör verksamheten?
- Vilka blir konsekvenserna?
- Vem har tillgång?
- Vem driver systemet på kort och lång sikt?
- Hur ser underhållsplaner ut?
- Vem är ansvarig för helhetsbilden?



Utmaningar ur ett förvaltningsperspektiv

Verkligheten



- 5 - 6 olika system i en park
- Administrativ hantering
- Åtgärder för teknisk & fysisk säkerhet

- Vad händer om något av dessa fallerar?

Utmaningar ur ett förvaltningsperspektiv

Hackad

- Låsta system
- Oberhörig tillgång & styrning av anläggningen
- Skalskydd forcerat



- <https://sverigesradio.se/artikel/6826867> —> “(2017) Det gick att styra vindkraftverk utan lösenord”
- <https://www.svtplay.se/hackad> —> “Ett experiment där hackare lurar sig in på företag”
- Nästa steg? Vad borde vi ha gjort?

Utmaningar ur ett förvaltningsperspektiv



Proaktivitet

- Bygg hellre en grov plan B med åtgärder än ett enskilt fokusområde som är perfekt
- En obehörig behöver bara hacka ett system - kom ihåg att du måste försvara kanske 5 till 50 stycken
- Det handlar inte om OM utan NÄR
- Nästa steg? Vad borde vi ha gjort?



Lösningen för dig som ägare

Tre steg

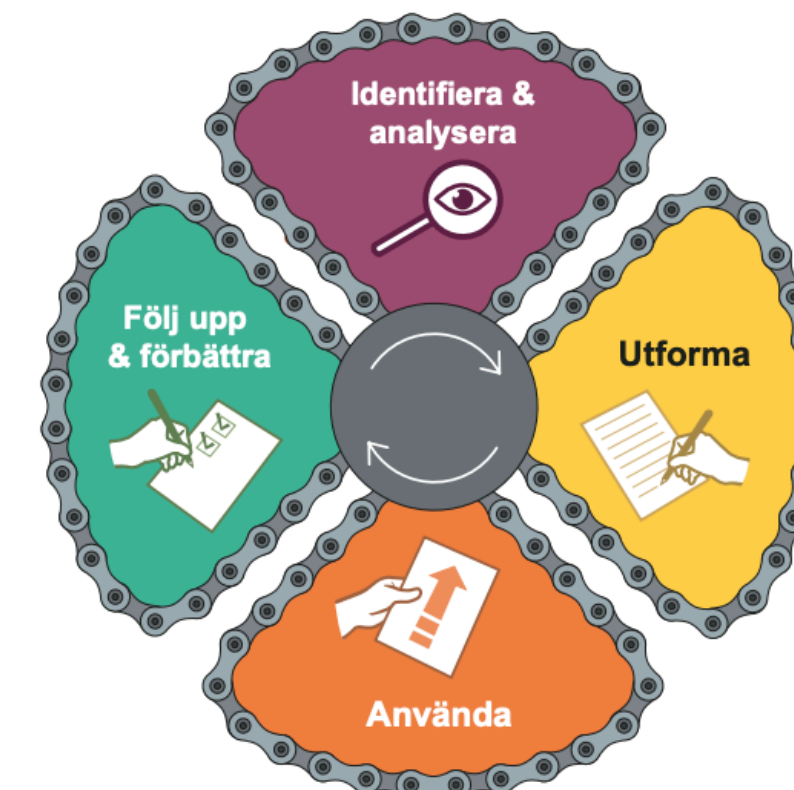
1. Seminarium - Hur påverkar detta mig & vår verksamhet?
2. Omvärldsbevakning - Vad händer inom området?
3. Systematiskt informationssäkerhetsarbete - Säkra din verksamhet!



+



+



Lösningen för branschen

Tre steg

- Sprida kunskap
- Samordna branschen
- Genomföra lagefterlevnad



Ett avslutande tips

<https://www.cert.se>



- Portal för att hantera och förebygga IT incidenter
 - Blixtmeddelanden
 - Bekräftade sårbarheter
 - Nyhetsbrev

The screenshot shows the CERT-SE website interface. At the top, there is a navigation bar with links for 'Om CERT-SE', 'Webbkarta', 'Sök', 'Om cookies', and 'Tillgänglighetsredogörelse'. The MSB logo and 'Myndigheten för samhällsskydd och beredskap' are also present.

NYHETER

- 2021-10-27 12:12**
Flera kritiska sårbarheter i Adobe-produkter
Adobe har släppt säkerhetsuppdateringar som hanterar flera kritiska sårbarheter i flera Adobe-produkter. Flertalet av dessa sårbarheter kan utnyttjas av en fjärrangripare för att köra godtycklig kod och ta kontroll över ett system [1].
- 2021-10-25 16:08**
Skadlig kod i UA-Parser-js
JavaScript-biblioteket UAParser (npm package), har distribuerat tre versioner innehållandes skadlig kod. Om du har installerat ett sådant paket bör du utgå från att systemet är komprometterat.
- 2021-10-22 12:56**
CERT-SE:s veckobrev v.42
Cybersäkerhetsmånaden rullar på med flera bra initiativ för att höja medvetenheten. SVT:s programserie "Hackad" bidrar med ökad kunskap mot allmänheten och när det gäller CERT-SE:s CTF så säger en bild mer än tusen ord.
- 2021-10-21 10:23**
Flera sårbarheter i Cisco-produkter
Cisco har släppt säkerhetsuppdateringar för flera sårbarheter, varav en anses allvarlig och har fått CVSS-klassificering 7.8 av 10 [1].
- 2021-10-20 10:35**
Oracles kvartalsvisa säkerhetsuppdatering för oktober 2021

INFEKTERADE DATORER I SVERIGE

576 infekterade datorer

The map shows the geographical distribution of infected computers in Sweden, with a high concentration of red dots in the southern and central regions. Labels for 'Norge Norway', 'Oslo', and 'Stockholm' are visible on the map.

IT-INCIDENTRAPPORTERING

Rapportering till följd av NIS-direktivet beskrivs på MSB:s webb:
<https://www.msb.se/sv/Forebyggande/Informationssakerhet/NIS-direktivet/>

Information om obligatorisk it-incidentrapportering för statliga myndigheter finns här:
<https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/it-incidentrapportering-for-statliga-myndigheter/>

Obligatoriet omfattar myndigheter, men även andra organisationer kan välja att rapportera frivilligt. Kontakta MSB/CERT-SE på cert@cert.se eller 0102-40 40 40. Vid användning av PGP-kryptering finns CERT-SE:s publika PGP-nyckel här.

PRENUMERERA PÅ BLIXTMEDDELANDEN

För att prenumerera på utskick från CERT-SE, ange din e-postadress i fältet nedan.

»

CERT-SE skickar ut blixtmeddelanden (BM) via e-post när det finns allvariga hot att informera om.

Det kan t.ex. gälla allvarliga säkerhetsbrister eller sårbarheter med uppmaning till omedelbara åtgärder för skydd.

Avsändaradressen för CERT-SE:s e-postutskick är bm@list.cert.se.

Mer »

Tack för oss!

Kontaktuppgifter



- Per Olofsson
- per.olofsson@w3e.se
- +46 70 510 72 82

- <https://www.w3e.se>



- Roger Klahr
- roger.klahr@infokontroll.se
- +46 76 118 63 46

Energy Security

Framtidens elproduktion säkras

Per Olofsson - 2021-11-01



W3 ENERGY