Hacking wind farms

Silverskin

JANI KIRMANEN, CDO
6.2.2025

Silverskin Information Security Oy

Silverskin is an information security company specialized in offensive security testing.

We help organizations to embed security into their digital development processes and to timely assess the security of constantly changing digital applications.

As a result, our customers can achieve optimal level of cyber security based on increased situational awareness and risk knowledge. In addition, they improve their security and product quality, reduce unexpected expenses, and meet business requirements.

1.9 M€	100+	300+	91	27	2009
Revenue	Corporate customers yearly	Customer assignments yearly	NPS 2023	Employees	Established

Past wind farm (and related) attacks

ATTACK	ATTACK VECTOR	IMPACT
Nordex Cyberattack, 2022 **IT System Breach**	External network exposure through IT infrastructure	Nordex, a major wind turbine manufacturer, detected unauthorized access to its systems and had to shut down IT operations globally to contain the breach.
Deutsche Windtechnik, 2022 **Ransomware Attack** **Remote Access Exploited**	Compromised external-facing remote access systems	The attack forced the shutdown of remote control for 2,000 wind turbines, though local operations continued.
Viasat Satellite Hack, 2022 **Supply Chain Weaknesses**	Cyberattack on Viasat's KA-SAT satellite, affecting communication infrastructure	5,800 wind turbines in Germany lost remote communication capabilities, making monitoring and control impossible.
Vestas Ransomware Attack, 2021 **Data Exfiltration & Extortion**	Ransomware exploiting IT system vulnerabilities	Attackers exfiltrated sensitive internal and employee data from Vestas' IT systems. While wind turbine operations were not disrupted, leaked information included personal data, bank account details, and social security numbers
Wind Farm Technician Malware Incident, 2018 **Phishing/Human Error & Malware**	Phishing/malware via an external, unsecured device	A wind farm technician unknowingly downloaded malware on a personal laptop while at a hotel. The next day, upon connecting this laptop to the wind farm's internal network, the malware spread, disrupting turbine operations

Top 5 security challenges for wind farms

1 REMOTE ACCESS VULNERABILITIES	Many operators use VPNs, remote desktop protocols (RDP), or cloud-based SCADA—all of which are prime targets for hackers. Attackers exploit weak credentials, unpatched vulnerabilities, or phishing attacks to gain unauthorized access.
2 SCADA & INDUSTRIAL CONTROL SYSTEM (ICS) SECURITY RISKS	Many SCADA/ICS systems were not designed with cybersecurity in mind and may have outdated security protocols. If compromised, an attacker could shut down turbines, manipulate power output, or cause grid instability.
3 SUPPLY CHAIN & THIRD-PARTY RISKS	Many operators depend on third-party vendors for maintenance, software updates, and cloud services. A compromised supplier or cloud provider can become an entry point for cyberattacks. An attacker targeting a SCADA software vendor could distribute malware to all wind farms using
4 RANSOMWARE & DATA EXTORTION THREATS	Operators store critical operational data, including turbine performance and grid integration details. Ransomware groups encrypt or steal sensitive data and demand payment to restore access.
5 COMMUNICATION & SIGNAL INTERFERENCE (JAMMING & SPOOFING)	Wind farms rely on radio, microwave, and satellite communications for monitoring and control. Attackers can use RF jamming, GPS spoofing, or signal interference to disrupt turbine synchronization and grid integration.

Importance of understanding attack surface

BEFORE INTELLIGENCE GATHERING

AFTER INTELLIGENCE GATHERING

Offense informs defence

"If you don't know what you have, you cannot secure it."

RICK HOLLAND

"Prevention is ideal, detection is a must."

DR. ERIC COLE

"The only constant in life is change."

HERACLITUS

SILVERSKIN
INFORMATION SECURITY OY
COMPANY ID 2296092-6
KALEVANKATU 6
00100 HELSINKI
FINLAND

silverskin.com