CASE-STUDY

Cyberattack on renewable Energy sector leads to widespread power outages

A case study of "GreenPower", a key broker in the renewable Energy sector, targeted by a sophisticated cyberattack, disrupting power supply to over 100,000 households

As a critical intermediary between power producers and consumers, GreenPower's role in the energy supply chain made it an attractive and vulnerable target for cyber criminals.

This breach not only highlighted the importance of cybersecurity in the energy sector but also underscored the potential for widespread disruption when key infrastructure nodes are compromised.

ABOUT GREENPOWER

Green Power Denmark is a non-commercial business organization gathering around 1,500 members from across the green energy value chain.

- Company size: Medium Enterprise
- Industry: Renewable energy industry
- Location: Denmark

ABOUT THE ATTACK

Hackers exploited a known vulnerability (CVE) in an outdated firewall within GreenPower's network.

This breach allowed them unauthorized access to the company's infrastructure. Leveraging GreenPower's connections to various power producers, the attackers navigated through interconnected systems.

Their ultimate target was the control center responsible for managing the power grid. Successfully infiltrating this control center, the attackers executed a critical strike – shutting down power to over 100,000 households.

THE SOLUTION

To address vulnerabilities and prevent future incidents, a multi-faceted approach was adopted:

- **XDR Platform:** Introduction of an Extended Detection and Response platform with AI for automated threat remediation and alerting.
- **Network Traffic Analysis (NTA):** Deployment of NTA tools to monitor and detect suspicious patterns in network traffic.
- **Endpoint Detection and Response (EDR):** Implementation of an EDR solutions to isolate and contain threats at the device level.
- **Deception Technology (DR):** Use of deception technology to trap, mislead and study attackers through decoys within the network.

THE PROBLEM

Several key issues facilitated this attack:

1. **Unpatched Firewalls and Systems:** Critical security patches were not applied, leaving known vulnerabilities open to exploitation.
2. **Shadow IT:** Unofficial and unmonitored IT systems or software were present, creating blind spots in security.
3. **Lack of Advanced Security Tools:** Absence of Extended Detection and Response (XDR), Security Information and Event Management (SIEM), or any robust alerting platform made early detection of the breach impossible.
4. **No Micro-Segmentation:** There was no separation in the network between GreenPower and the power producers, allowing the attackers to move laterally with ease.

The GreenPower incident serves as a stark reminder of the importance of cybersecurity vigilance, especially in critical infrastructure sectors. The comprehensive measures adopted in the wake of the attack not only rectified immediate vulnerabilities but also set a new standard in network security for the energy sector.