

# Cyber risks from a whitehacker's perspective

Internetwache.org  
Sebastian Neef & Tim Philipp Schäfers

June 7, 2017



## Internetwache.org

A secure internet is our concern

### About the project

- Responsibly disclosing vulnerabilities since 2012
- Recent focus on “critical” infrastructure like Operational Technology (OT) and Industrial Control Systems (ICS)

# Critical infrastructure?

Our research revealed ...

- Waterworks in Germany and Italy
- Mobile traffic lights in Germany
- Clinic Systems in Switzerland
- Smart Buildings / Smarthomes

... unprotected and accessible on the internet!

# How does that look like?

**Hauptpumpe 1**  
Wahlschalter Automatik  
Wahlschalter Hand  
FU betriebsbereit  
FU Netzschütz ein  
FU Schütz ein  
Netzschütz ein  
Regelbetrieb

**Hauptpumpe 2**  
Wahlschalter Automatik  
Wahlschalter Hand  
FU betriebsbereit  
FU Netzschütz ein  
FU Schütz ein  
Netzschütz ein  
Regelbetrieb

**Tastatur**  
2950 U/min

7 8 9  
4 5 6  
1 2 3  
- 0 .

HP1 Reglerausgang: 100.0 %  
Drehzahl: 2950 U/min  
HP2 Reglerausgang: 100.0 %  
Drehzahl: 1 U/min

Monat: 4039 m³  
Jahr: 72145 m³

Sollwert Druck: 0.00 bar  
Istwert Druck: 5.25 bar

Verbrauch ON  
Vortag: 513 m³  
Tag: 361 m³  
Monat: 3236 m³  
Jahr: 58402 m³

# Why does that happen?

Three major problems:

- Law and Regulation
- Point of Contact and Communication
- Complex IT-Security Guidelines

Demo!

# Live hacking!

# Q&A

Thank you for your attention!

- Questions?
- Discussion?

# Backup

← ⓘ 🔒 | <https://www.google.ch/search?client=psy-ab&site=8&source=hp&btnG=Suche&q=wind+farm+portal>

**Google** wind farm portal 🔍

[Alle](#) [Bilder](#) [News](#) [Maps](#) [Videos](#) [Mehr](#) [Einstellungen](#) [Tools](#)

Ungefähr 2'610'000 Ergebnisse (0.62 Sekunden)

Tipp: **Begrenze die Suche auf deutschsprachige Ergebnisse.** Du kannst deine Suchsprache in den Einstellungen ändern.

**[PDF]** [nordex control 2, das wind farm portal](#)  
[www.nordex-online.com/fileadmin/MEDIA/Sonstiges/Nordex\\_Control\\_2\\_DE.pdf](http://www.nordex-online.com/fileadmin/MEDIA/Sonstiges/Nordex_Control_2_DE.pdf) ▾  
Wind Farm Portal® Nordex Control 2: Hier werden die Daten einzelner Windenergieanlagen, der meteorologischen und betriebsführenden Systeme, des ...

**[PDF]** [nordex control 2 wind farm portal](#)  
[www.nordex-online.com/fileadmin/.../Nordex\\_Control\\_2\\_EN.pdf](http://www.nordex-online.com/fileadmin/.../Nordex_Control_2_EN.pdf) ▾ [Diese Seite übersetzen](#)  
management and long-term system maintenance after delivery and integration of the system. The Nordex Control 2 Wind Farm Portal® registers all the data.

**Nordex Control - Wind Farm Portal (ver. 11.06.13 ...**  
[193.253.196.156/](#) ▾ [Diese Seite übersetzen](#)  
Wind Farm Total Summary. Wind Farm Handover, 24.09.2007. Number of Turbines, 4 (4). Total Production, 143465.72 MWh. Data Availability, 99.43 %.





# Backup

The screenshot shows a web browser window displaying the Nordex NC2 Wind Farm Portal. The browser's address bar shows the URL `217.86.374.302/32_95_03/index_en.jsp`. The page features the Nordex logo and the title "NC2 Wind Farm Portal".

**Nordex Control Login**

Certificate  Secure  Basic

Username

Password

Login

**Select Language**

Language

**Wind Farm Total Summary**

Wind Farm Handover	05.04.2012
Number of Turbines	8 (8)
Total Production	296311.38 MWh
Data Availability	100.00 %
Availability	97.80 %
Capacity Factor	34.30 %
Mean Wind Speed	7.0 m/s

# Backup

view-source:http://217.86.174.101/13\_05\_01/index\_en.jsp

```
1
2
3 <html>
4
5 <head>
6 <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
7 <link rel="stylesheet" href="index_en.css" type="text/css">
8 <title>Nordex Control - Wind Farm Portal (ver. 13.05.01) Behrendorf</title>
9 <script src="language.js" type="text/javascript"></script>
10 <script src="errors.js" type="text/javascript"></script>
11 <script type="text/javascript">
12     function init() {
13         if (!checkCookieSupport()) {
14             alert("Cookies must be enabled to use Nordex Control");
15         }
16         if (isCertificateUsed()) {
17             document.getElementById("deactivated").style.display="";
18             return;
19         }
20
21     var lang = getLanguage();
```

# Backup

intitle:"Nordex Control - Wind Farm Portal"

Google

intitle:"Nordex Control - Wind Farm Portal"

Alle News Bilder Maps Videos Mehr Einstellungen Tools

Ungefähr 103 Ergebnisse (0.40 Sekunden)

## [Nordex Control - Wind Farm Portal \(ver. 11.06.13 ...](#)

[193.253.196.156/](#) - Diese Seite übersetzen

Wind Farm Total Summary. Wind Farm Handover, 24.09.2007. Number of Turbines, 4 (4). Total Production, 143465.72 MWh. Data Availability, 99.43 %.

## [Nordex Control - Wind Farm Portal \(ver. 13.04.00\) Roth\\_Rock](#)

[63.88.1.54/](#) - Diese Seite übersetzen

Wind Farm Total Summary. Wind Farm Handover, 06.12.2010. Number of Turbines, 20 (20). Total Production, 464810.66 MWh. Data Availability, 99.83 %.

## [Nordex Control - Wind Farm Portal \(ver. 11.06.13\) Wulfdiek](#)

[217.86.216.154/](#) - Diese Seite übersetzen

Wind Farm Total Summary. Wind Farm Handover, 19.09.2011. Number of Turbines, 5 (5). Total Production, 104756.59 MWh. Data Availability, 100.00 %.

## [Nordex Control - Wind Farm Portal \(ver. 13.05.01\) Behrendorf](#)



# Backup

