ROLKEN

BLACKOUT - A THREAT MODELING

For power generation and distribution, there are known threats like under or over voltage, system stability, and environmental risks. In addition, there are unknown risks related to technological advances. These include targeted attack, crypto jacking, communication interruption or attack on third-party assets connected to the grid but out of direct control like renewable resources.

OBJECTIVE

1. find out whether it is possible to trigger power outage that would account for about 1.4 million supply points;
2. focus on realistic and domain-specific threat scenarios (separation between brownout and blackout);
3. separate threats to OT technology, grid-related threats, integration, communication, and third-party threats;
4. selected threats with high-probability will be subject to mathematical simulation.

ABOUT THE CLIENT

A multinational energy company with assets in power generation, distribution, and renewables. The internal technological landscape consists of multitiered SCADA control centers and over 10 vendors of OT technology. Distribution grid connects over 2000 renewable resources.

CHALLENGE

Preparing **a realistic scenario** required domain expertise in power generation and distribution, knowledge of technological (OT) systems and integration to IT systems.

Another challenge was to prepare mathematical models for blackout simulation and calculation of network effects.

RESULT

The company has accepted threat models on a group-wide level and implemented changes to risk plans. As a result, we tested selected top 5 five threats with mathematical models in physical grid simulation polygon. For this reason, the company had changed **five-years strategy and crisis planning.**

At the same time, average **saving** when purchasing new technology increased by **6%** due to clear risk models. The average **speed of procurement increased by 14%** because of shorter selection criteria due to changes in the security strategy.

HOW WE DID IT?

DOMAIN EXPERTISE

We gathered to our “war room” domain experts in the field of power generation and distribution, business consultants and integration experts, hackers and mathematicians. As a result of this know-how, we created long-list of threats.

TECHNOLOGY ANALYSIS

We did not differentiate between OT and IT assets. Technology is technology and could be abused. Instead, we created a threat model based on internal characteristics, role in deployment, criticality and analyzed distance from a process (e.g. power generation).

STRICT SELECTION PROCESS

Shortening long-list was the most crucial part of the project. We discarded 85% of items on long-list to focus only on high-priority threats.

UKNOWN-KNOWS

The things you think you know, that it turns out you did not – these were winners in this threat modeling. Renewables which can be controlled remotely, radio communication, optical communication lines.

MATHEMATICAL MODELING

Selected three biggest threats were the subject of mathematical modeling. For example, we used Wolfram Mathematica to create distribution grid simulation. Based on calculations and data from our scan of internet IPv4 range we modeled take-over of 100% of biggest renewable resources in the distribution grid and started changing output characteristic.

ROLKEN

HAVE ANY QUESTIONS? INTERESTED? GET IN TOUCH!

CALL US +420 228 224 645, DROP US EMAIL ON HELLO@ROLKEN.CZ