Ir. Max Kerkers
is a manager at KPMG Cyber & Privacy.

Drs. Pieter de Meijer RE CISSP CISA
is a director at KPMG Cyber & Privacy.

Ir. Ronald Heil
is a partner at KPMG Cyber & Privacy.

Security of Smart Grids: a neglected issue

For a green future, energy grids need smart solutions to match demand and response. These Smart Grids offer fantastic opportunities, but their cyber security risks need adequate attention. This is not always the case. Governments, grid operators, energy producers and everyone else involved have to work even harder to make this happen. Technical security is already receiving due attention, but that's not enough. In this article we will look at the possible solutions to reduce cyber risks and prevent damage if an incident occurs.

INTRODUCTION

The energy transition is particularly demanding on the Dutch power grid. Increasing electrification requires more and more capacity and (many) more connections for solar panels, wind turbines and all kinds of other local energy initiatives. A traditional approach to this challenge - for example, by continuing to expand the grid - is becoming unaffordable, which is why Smart Grids are a good idea. These are technological solutions that help the demand for energy to evolve along with supply, limiting the additional pressure on the grid. Smart Grids make it possible to green our society at the pace we envision.

One of the important prerequisites for the successful implementation of Smart Grids is that they are also properly secured. The good news in this regard is that grid operators are often (partly) still in the design phase of these Smart Grids. This means that there will be plenty of room to create the context necessary for Smart Grids to also function securely.

Unfortunately, there is also less good news: opportunities to build a sound foundation for (cyber)secure Smart Grids are now barely used. That foundation requires identifying risks and taking effective measures, whereby we consider that things do go wrong and how we can minimize that impact. That foundation can only work if we know who the parties connected to Smart Grids are, and if it is possible to manage the joint securing of Smart Grids.

The fact that this foundation is only laid to a limited extent is partly because cyber security is not solely the responsibility of grid operators. On the user side, they only have limited control over the degree of cyber security. Think of electric cars and their charging stations. Or industrial sites with their own energy generating capacity using solar panels and wind turbines. In addition, concerns about growing interconnectivity and the potential for malicious actors to take advantage of it loom large. What needs to be done to prevent these Smart Grids from turning out to be not so smart after all?

Hackers, whether or not employed by hostile states or criminal organizations, are increasingly making the digital world unsafe

Solutions are available but, even though these solutions are increasingly on the agenda in the energy transition, it is hugely complex to digitize an existing (physical) network in an existing ecosystem. In that complexity, cyber risks need to be taken seriously and structurally addressed. This requires political will and direction combined with collaboration in the chain between private and public parties.

In this article, we discuss the solutions for identifying cyber risks, preventing them and mitigating the impact should a cyber incident occur.

CYBER RISKS ARE A REAL THREAT

Cyber risks are not imaginary, which has become evident. The Russian attacks on Ukrainian energy networks before the war in Ukraine broke out, the cyber attacks during the war in 2022 and 2023, and the ongoing aggression toward (large) companies with ransomware are just a couple of examples. Hackers, whether or not employed by hostile states or criminal organizations, are increasingly making the digital world unsafe. When it comes to energy networks, this can have nasty consequences on several fronts. Five are described below.

1. Blackouts. Parts of society are left without power, heat or other forms of energy. The effect can be disruptive.
2. Physical consequential damage. Parts of the infrastructure can be destroyed or people purposefully disrupt energy supplies at vital locations, such as hospitals. This can result in deaths or injuries.
3. Technical disruptions. More technology-oriented disruptions such as shifting grid frequencies that cause digital clocks to stop synchronizing. Older devices in particular break down as a result, which can lead to (high) costs, inefficiencies, delays and other inconveniences.
4. Financial damage. Reduced energy availability, such as from blackouts and disruptions, can lead to higher energy prices. Households therefore have less money left over to spend on other things and may run into financial difficulties. This is not inconceivable, considering the current geopolitical situation.

5. Privacy violations. Because Smart Grids are very fine-grained, with multiple connections into consumers' homes, the information exchanged over those networks can be privacy sensitive. For example, whether residents are home or not can lead to damage (intrusion).

Some characteristics of Smart Grids also make this type of network even more susceptible to cyber risks than other networks. The number of contact points is increasing, as is the number of connections and the extent of interaction between all these components. All in all, the so-called attack surface is becoming a lot larger. Identifying relevant threats, and certainly the vulnerabilities of one's own organization and infrastructure, should therefore be part of the implementation of Smart Grids.

Managing, mitigating or eliminating those vulnerabilities should be a focus point as early as the design of Smart Grids. Preventive measures will be central, complemented by the right measures to detect threats and actions that can limit the impact from attacks.

PREVENTIVE MEASURES TO REDUCE THE LIKELIHOOD OF A CYBER INCIDENT

In terms of prevention, the most important solution is to provide secure standards for setting up Smart Grids. Such standards are lacking now. Almost every party takes a different approach to cyber security, and this results in series of vulnerabilities. We advocate cooperation among the major market players - encouraged by the government - to develop such a secure standard and be mandatorily adopted by the entire industry.

Importantly, this involves an "ecosystem" of stakeholders in the energy chain. The standards should not only apply to the grid operators; the complexity in this playing field is too great and the security issue will not be solved by simply demanding more from the grid operators. In addition, it has become clear in recent years that the energy transition has required and will continue to require substantial financial investments from grid operators. It is time for the security burden to be borne by more shoulders.

In line with this, a second important solution to the cyber risks of Smart Grids is a greater guiding role of the government. The current European directive (the NIS Directive) for the security of critical infrastructure is implemented in the Netherlands with the Wbni (Wet beveiliging netwerk- en informatiesystemen, *Security of Network and Information Systems Act*). However, compliance is lacking and not adequately monitored. Many organizations view such laws and regulations from a compliance perspective: doing it because they have to and not from an intrinsic motivation. As long as the "stick" is insufficiently used, the need to do something is moderate. To date, supervision is still limited, partly because it is organized by sector and because supervisors are dealing with scarce capacity to conduct audits and supervision.

Given the importance of Smart Grids for our green future, this is an undesirable situation: tighter government direction is needed. An additional advantage is the recently issued successor to the NIS Directive: the NIS2.

Although the content and approach are largely similar to that of the current NIS Directive, it is to be expected that NIS2 will be less non-binding and more "prescriptive" on a technical level. Fines associated with increased enforcement, at least on paper, are not negligible. They can be as much as 10 million euros or 2 percent of global turnover. The fact that the energy sector is considered "critical" from a regulatory perspective should come as no surprise. After all, without energy supply, a lot of essential services in a country will come to an immediate halt.

The NIS Directive (NIS stands for: Network & Information Systems) is European legislation aimed at increasing the cyber security and resilience of critical systems in Europe. It is up to the European member states to translate the Directive into national legislation. In the Netherlands, the Wbni was established, with supervision assigned to the Dutch Authority for Digital Infrastructure (*Rijksinspectie Digitale Infrastructuur, RDI*), formerly known as the Agentschap Telecom. The NIS2 Directive is the successor to the NIS Directive and came into force in early 2023. The elaboration of NIS2 for the Netherlands will take effect later in 2023; the deadline for member states is October 2024. Organizations covered by these regulations must comply with the requirements by January 2025 at the latest. The energy sector in a broad sense has already been designated as a "critical infrastructure" under the NIS Directive. This will be further extended with NIS2 towards the underlying ecosystem.

It is expected that the supporting and supplying companies of the energy sector also have to deal with the NIS2 requirements to a greater extent. It will take some time to establish enforcement in the Netherlands and gather the necessary experience and capacity.

A third preventive measure to prevent attacks on (future) Smart Grids is to certify the network devices consumers use. Having a sound and uniform certification system in place will assure consumers that there is no malware in the equipment and that it cannot be exploited from the outside.

DAMAGE CONTROL AFTER AN INCIDENT

Cyber risks must have a place in the plan and design phase of Smart Grids

In addition to preventive measures, the application of Smart Grids will also be more secure if governments, grid operators, energy producers, businesses and consumers take action to mitigate impact should unexpected incidents occur. This involves, first of all, building more buffer capacity, for example, with industrial batteries of significant capacity (think of a supply capacity of 100 megawatts). While one of the main advantages of using Smart Grids is that it is the very reason why there is no need to massively expand the capacity of networks, from the point of view of security it is also not recommended to remove all leeway in terms of fallback options. The presence of buffer capacity reduces the impact of a cyber incident by allowing energy supply to continue for longer.

Broader cyber risk management - which may include building buffers - should additionally assure organizations and consumers that the consequences of incidents will be contained. Cyber risk management provides structured detailing of threats and vulnerabilities, leading to a picture of relevant risks. For each risk, it is necessary to consider the measures (preventive, detective, repressive or corrective) that are effectively needed to mitigate the risk.

Knowing what can happen is a prerequisite for this, and scenario development will be used for this purpose. Next, we will need to describe the objectives. How long should a blackout last before the damage is insurmountable, which systems should be given priority for recovery, which parties will be given priority? Based on those objectives, roadmaps will be written. Exercises, preferably large-scale and based on attack simulations, should then reveal whether risk management is properly implemented.

GAINING AN OVERVIEW OF THE PLAYING FIELD

One of the biggest challenges in this regard is national coordination. It is already difficult to get a clear overview of all points connected to the Smart Grid, because high-volume consumers connected to the Smart Grid have a notification requirement, but private initiatives can connect to it without any notification requirement. The collection of grid operators, high-volume consumers and private individuals combined with modern Internet of Things and Smart Grid functionality on the same grid makes the security issue complex. And, for each point (organizations, companies, charging points, solar parks, et cetera), it must be clear which security measures have been taken. An additional battery at neighborhood level or additional energy production at a hospital, can all affect the risk management to be put in place at national level. The problem is that the responsibility for those local and regional measures always lies at decentralized level. In our view, grid operators should play a greater role in this. In the digitalization of grid operators' infrastructure, for example where substations are concerned, security is already receiving the necessary attention in recent years. The complexity and lack of clarity in "governance" are greater in the area of private Smart Grids (for example, in a business park) and within developments in "smart cities," where citizens and government must work together, than in Smart Grids solely utilized by the grid operators.

COOPERATION BETWEEN ALL PARTIES IS INDISPENSABLE

Similarly, the cyber risks of Smart Grids are another reason to prevent the fragmentation of the Dutch energy supply. This is not an impossible task, but it is imperative that all stakeholders quickly choose the path of cooperation. This has to be a far-reaching and intensive collaboration, with security high on the agenda. It is more common in IT that projects seem to revolve solely around functionality, but when it comes to the construction and implementation of Smart Grids, the Netherlands cannot afford that. These smart grids are potentially a wonderful solution to one of the biggest challenges of the energy transition. However, it will prove impossible to deliver on that promise if crucial preconditions such as compliance, risk and cyber security are insufficiently addressed.

That is why now is the time, in the plan and design phase of Smart Grids, to incorporate the cyber risks of these smart grids integrally into those plans and designs. As we described above, standardization, certification and a greater guiding role for the government should make this possible, along with insight into who the connected parties to the Smart Grids are, and with structured cyber risk management. The grid operators are taking the necessary steps in this regard. The challenge now is to also take these steps in Smart Grid developments outside the grid operator's infrastructure.

About the authors

Ir. Max Kerkers is a manager in the Cyber Assessments team at KPMG Cyber & Privacy, where he helps clients gain insights into the security of their OT environments. He advises them on how to better protect these often-critical environments from cyber threats in a practical way.

Drs. Pieter de Meijer RE CISSP CISA is a director at KPMG Cyber & Privacy and has extensive experience in information security and compliance. He has advised various organizations on structurally improving their ability to secure their information.

Ir. Ronald Heil is a partner at KPMG Cyber & Privacy and specializes in the secure transformation of IT and OT environments, and specifically the security of OT environments. He also has a role at KPMG as a global leader for risk advisory in the energy domain.