REACTIE SMA:

In general, we want to stress that the attacks described by Willem Westerhof are only possible, when the attacker is already INSIDE the local home network. This means, that he would first have to have hacked/bypassed the various routers/firewalls of PV system owners to a considerable extent. Such an attack on the router/firewall is extremely difficult to perform, and it would provide the hacker with access to many other devices and confidential information within the local home network.

ITsec: Note that attacks to gain access to the local home network are a growing problem. From a hackers perspective there are many ways you do this. Examples are vulnerable routers, IP-camera's and unprotected or badly secured WiFi-networks. Such an attack is not very difficult to perform. It takes time and/or money. Our suggestion is to immediately stress the importance of the security of PV-installation and that SMA, since Willem's research, is working continuously to improve the level of security of its devices and security within the PV-industry in general.

How many SMA-inverters are being in operation in The Netherlands? And how many in Europe?
Due to competitive reasons, we generally don't disclose these numbers. In addition, from our extensive product portfolio, only the following SMA inverter types are affected by Willem Westerhof's report: Sunny Boy models TLST-21 and TL-21, Sunny Tripower models TL-10 and TL-30, and of these, only the approximately 25 percent of all inverters that are directly connected to the internet might be affected. This makes only a small portion of all installed SMA inverters. We want to stress that even with the inverters mentioned above, the assault vectors require extremely high efforts and extensive expertise by a potential hacker. Even the devices mentioned above are properly protected from hacker attacks, if the users carefully adhere to the measures outlined in our public cyber security guidelines, which are delivered with each inverter that leaves our production and are also published on our Website (please see http://files.sma.de/dl/7680/CyberSecurity-TI-en-10.pdf). Any device not connected to the Internet is generally not affected. As already mentioned above, this also applies to devices connected to a router with a firewall, which is the case for almost all residential installations.

ITsec: We think that SMA devices are, compared to other manufactures, relatively secure. The test of Willem was a Proof-of-Concept. We expect that devices of other manufacturers are less secure and will show similar vulnerabilities.
The number of connected inverters is growing every day. Also inverters that are not connected to the internet are vulnerable for (targeted) attacks. We believe that for example an attack exploiting BlueBorne using Bleutooth bases

viruses and worms can be used.
The guidelines issues by SMA are very good. We believe that for an average home users the are rather complex. But this is not only a task of SMA also the government and other stakeholders in the industry like the home users themselves have a responsibility.

2. How much giga-watt is running through SMA in The Netherlands? And how much in Europe?
As mentioned before, we generally don't disclose detailed numbers on a country-base. Overall, in the Europe, Middle East and Africa (EMEA) region, SMA has a total installed base of more than 35 GW. This includes not only small inverters for households, but inverters for all plant sizes, from small households through to multi-megawatt solar parks. As mentioned above, only a small portion/ few specific models of our inverters for households, that are directly connected to the Internet, might be affected.

ITsec: Note that Willem's scenario was not limited to SMA-devices. Scientifically, a loss of 3-4 GW is enough to cause dis balance in the grid. In the above scenario a 10% (approximately) install basis is enough.

3. What has SMA done with the findings of IT-Sec since their first hack in 2016, to improve the safety of inverters?
We have taken action immediately. Willem Westerhof published his report in August 2017. SMA has then immediately analyzed the publication and published a whitepaper on the findings and assessments (please see https://www.sma.de/fileadmin/content/global/specials/documents/cyber-security/Whitepaper-Cyber-Security-AEN1732_07.pdf).
A software project has been started to provide fixes for the various inverters. Additionally, we designed a new encryption protocol for inverters so that not only the communication to the Internet (which already is encrypted), but even the communication WITHIN a home network is encrypted. Currently, we are in the certification and deployment process so the patches and latest firmware version can be deployed to affected devices.

ITsec: We suggest more 'transparency' in de PV-industry. After Willem's disclosure SMA immediately started working on patches. This has taken quit some time. This has to do with resources (security team) and the nature of the devices (deployment). SMA should have been more transparent about this.

In general, security of the energy network has the highest priority for SMA. For every product type, risk assessments are executed, including penetration tests by independent security consultants. Additionally, SMA employs a dedicated

group of security experts with high competence in security of embedded devices. We are also participating actively in important security-related organizations like the SunSpec Alliance and SolarPower Europe.

4. Why does it take such a long time before action has been taken?
SMA has prepared a set of patches which have to be distributed in sync, because we have made essential changes to the fieldbus communication, which require all communication devices to be compatible with.
Moreover, for changes of the inverter software there is a certification process necessary (which is related mainly to electrical safety issues). This takes a noteworthy time. When released, the firmware will be deployed automatically to each device by using a secure channel.

ITsec: See previous remarks.

5. Has SMA informed their consumers/installers of its vulnerability?
Yes, we have informed our customers with a customer letter as well as on our website and on our corporate blog. We have also published a comprehensive whitepaper on cyber security with our answers to Willem Westerhof's statements through these channels. (Please see link in answer 3.).

ITsec: We think the white paper helps a lot and is one of the necessary steps to raise awareness and improve the security of PV-installations. This is in every bodies interests.

6. Has SMA consulted network-operators or industry peers?
Yes, we have conducted risk assessments with grid operators and peers from neighboring industries based on Willem Westerhof's report and our whitepaper. In addition, we have explained our security concept to several national cyber security agencies (including the Dutch National Cyber Security Center (NCSC)) without receiving any obligations.

ITsec: We think this is very important. For the future we hope the PV-industry will impose a security standard (self regulation). We are talking to SMA and Solar Edge to actually realise this.

7. Does SMA recognize that it is still possible to hack the inverters?
As already mentioned in the beginning, Willem Westerhof's attack scheme is only applicable when the attacker is already inside the local home network, and the assault vectors require extremely high efforts and extensive expertise by a potential hacker. We also acknowledge that there will never be absolute security, as is shown by numerous examples in other sensitive industries. SMA responds to this by constantly evolving its security measures, and we are

convinced that, if owners of the affected inverters adhere to our security guidelines, a successful hacker attack is nearly impossible.

ITsec: See our first remark. SMA and the PV-industry should not underestimate the risk.

8. What will SMA do with these findings?
As mentioned before, we are constantly working on continuous improvement of security standards that have to take pace with the rapid technological development. In general, cyber security is an extremely important topic that needs to be permanently addressed. With our firmly established processes and measures we make sure that our products and solutions always adhere to the highest IT security requirements and international standards. An interdisciplinary team is permanently working on secure system solutions and their integration – starting from product development and reaching to regular remote updates of our inverter software in the field.

ITsec: We would like to stress that SMA in our recent meetings takes a more proactive role and takes responsibility. It has taken too long to get to this point. It would have been better that SMA had been more transparent and less defensive from the start.

9. How does SMA look at the risks that comes with the vulnerability of the converters?
The security of our devices has highest priority for SMA in all respects and we do everything we can to protect our inverters and communication products against cyber-attacks. We are continually working on implementing the highest security standards and measures with our devices in order to make them as invulnerable as possible to attacks. We also make our customers aware that it is important for them to adhere to our cyber security guidelines. With these measures in place, the risk of a successful hacker attack is minimal.
|
Tsec: The risk we are talking about is not the sole responsibility of the users nor the manufacturer. SMA has a responsibility to produce inherently secure devices the users has to apply the devices securely. Also other stakeholders have distinct responsibilities.

10. How real does SMA consider the scenario that the power grid can be brought in imbalance?
In general, decentral power production makes the grid much less vulnerable to hacker attacks than central power production as a lot of decentral devices have to be attacked at the same time, which is rather complicated and takes a lot of knowledge, effort and resources. Even in the extremely unlikely event

that the affected SMA inverters in the field should be hacked successfully at the same time, we see absolutely no danger to grid stability, because they make only a small portion of all inverters sold by SMA and they are installed all over the world within different time zones.

ITsec: This is true if all decentralised power production is secured properly. In reality we believe this is not the case (yet). We can imagine certain actors (terrorists, states) have the time, money and resources for a large attack. As mentioned before, this has to be taken seriously.

11. What would it cost to apply protection to inverters - for both company and consumer?

As we have outlined before, we are constantly working on implementing the highest security standards and we also ask our customers for their support, as the highest security standards can only be achieved, if we work hand in hand. A securely configured router/firewall is the best protection for a secure integration, and the updates for SMA devices are provided automatically for free.

ITsec: See previous remarks.