Siemens Grid Software Podcast <de>coding the future of energy – Episode 6: How to make the grid <cyber>secure | with Kiersten Todt and Natalia Oropeza

Speaker 1
A: Hello, Mrs. Betge. Please have a seat. What can I do for you?

B: Thank you, Mr. Grünheide, for having time on such short notice.

A: Not much, actually. We just wanted to inform you of an arrest.

B: An arrest. And why are you coming to me with this?

A: It's regarding a former employee of your administration who was fired for data misuse a few years ago. There was also a lawsuit at the time which he lost. For investigative reasons, I'm not allowed to tell you the name yet. He must have felt he was treated unfairly and tried to take revenge.

B: Oh, that's, um. Hmm. I don't know what to say about that. My predecessor once told me that it had been a rather unpleasant incident. But what's actually happened now?

A: You've been the city's mayor for four years.

B: Four-and-ahalf years.

A: Exactly. And your predecessor expanded the smart power grid with the municipal utilities?

B: Yes. Nearly all of our citizens are simultaneously both electricity customers and producers in various ways. This was a key result of our “United Energy for All” agenda. It saves everyone a lot of money and makes us autonomous to a great extent.

A: And that's exactly what our perpetrator was after.

B: How so?

A: He planned to gain access to the central grid control, probably to shut down the grid and cause a widespread power outage. In fact, his approach was quite clever. But there was one thing he didn't know.

B: What's that?

A: It was probably not clear to him that all important partners are networked with each other via the cloud and that attacks on individual incidents could thus be identified not as individual cases, but as targeted action, and that your grid software provider immediately informed us when unauthorized access attempts were registered from similar IP addresses.

B: Ah, OK.

A: The profile of these attempts indicated without a doubt that an attack was imminent.

B: Hmm. It seems that we got off lightly and averted the crisis.

A: Let's put it this way. If network control still ran via your server like it used to, then you wouldn't have stood a chance. But via the algorithms in the cloud, your providers, I can detect these kinds of attack or espionage attempts early on via anomaly detection and monitoring. A standalone server can never access this intelligence. In fact, everything was done right many years ago, which helps us to prevent further issues today.

B: Hmm. I'm really relieved to hear that. You know, when our provider suggested that we move from the server to the cloud, the most common argument against it was that nothing protects against an attack better than steel and concrete.

A: Well, now we know at least that bits and bytes do a much better job.

Natalia: Ladies and gentlemen, this is Natalia Oropeza. I will be your host today to this old case of decoding the future, and I am so honored. I welcome our guests here, Kiersten Todt, the chief of staff at the Cybersecurity and Infrastructure Security Agency. So, Kiersten, welcome. And the floor is yours. I am sure you want to say hi to the audience and maybe introduce yourself as well.

Kiersten: Thank you so much, Natalia. It's great to be with you and I'm really looking forward to our discussion about energy and the future of energy. As you mentioned, I'm chief of staff of the Cybersecurity and Infrastructure Security Agency, which is an entity, a component within the Department of Homeland Security in the United States. We are America's Cyber Defense Agency. We're the newest federal agency, launched in 2018, but truly an aggregate of a lot of work and people and resources over many years that have focused on infrastructure protection, cybersecurity. And really, our role is to protect the functions of government and the private sector that are vital to the United States — he critical services that we rely on every day from the water we drink to the gas we get at the fuel pumps, to the electricity that lights our homes and businesses. So I very much look forward to this conversation as we dive deeper into electricity and energy.

Natalia: Thank you, Kiersten, again. And now tell me anything about what is in your mind these days. Anything could be private as well. Yeah. Tell me, anything that is in your mind these days.

Kiersten: Well, something that we've been talking about at CISA as we're looking to 2023 is, you know, we often talk a lot about the threat environment, which obviously is critical, and we manage the threat environment. But one of the elements of this that we understand is that the technology ecosystem is also a challenge. If we are not investing in security as we're building out the technology ecosystem, if we're not investing in secure by design, secure by default, ensuring that secure innovation — while some see that as a contradiction in terms — is actually an end state or actually a process, then we're going to miss out on the opportunity, but probably more importantly, we're going to be creating more vulnerabilities. So as we're looking at integrating technology innovation, that it's so important to be focused on how we're building this out with security as a priority.

Natalia: Right? I don't want us, cybersecurity in Siemens, to be seen as a person that says what people should do and what not to do, but rather I want us to be seen as a superhero because this is what you need these days to deal with the cybercrime. And from all the superheroes I know, Iron Man is my favorite. And the reason why this he's my favorite is because he uses technology with purpose. And in this case, the purpose that he has is to defend and to protect people in that he does by flying and looking at things that others cannot see. And I picture myself not flying but looking at things that others cannot see so that I can protect Siemens on time, which is a very important piece. So this is what was in my mind these days... I have to accept Kiersten. And with that, let's jump in to the topic and I would like to give the audience a little bit more background on what are we talking here about, why smart grids are so important. So smart grids are crucial to the sustainability of a modern society. Energy providers estimate that energy costs will rise by up to 400% in countries that do not set up smart grids. Only smart grids can ensure a stable energy supply against the backdrop of the energy and it is necessary to balance offers from an almost unimaginable number of small electricity producers electric electricity storage in the rapidly increasing demand from e-mobility and electricity or heating. So this is the background of the conversation that we are having today, this is how important smart grids are, and these are the opportunities that the societies will have by deploying them. So we do really want societies to use smart grids. Now, like everything like everything in life, opportunities and benefits, they come with some risk — and those risks we have to manage. And now, more specifically, I am referring to the cyber security risks, now with digitalization meaning with the smart grids, we are increasing the connectivity of devices that were not connected before, and those devices have vulnerabilities, therefore, the number of vulnerabilities will increase in these warsin this smart grid perspective. I have some studies that are showing that the number of devices connected in the digital world is growing almost exponentially, and accordingly the vulnerabilities are following the same, but meaning they are also growing... they are also growing exponentially. So if you multiply the number of devices you have in the digital world times the number of vulnerabilities and at least we know that 13% of them are critical, then you can imagine the risk I am here talking about. Now, to the audience, don't panic, because like always in life, what you need to do is to manage the risk. And this is the core of the conversation Kiersten and myself are having today here. So let me tell you a couple of aspects that you have to observe. You have to manage, number one, the inventory of the devices that you have connected. And this sounds really easy and really simple, but believe me, it's not always the case...that either the locations or the factories or the sites, they know exactly what they have connected to the. to the network, to the infrastructure, and they also don't know who the owners are,and if you don't know who the owners are, then of course you cannot manage their vulnerabilities on time, that those, those devices have. So, this is this is just to mention one of the topics that I would like to go in more detail, and then we'll pass to you, Kiersten, to to to help the audience imagine those kind of risks that could emerge from the use of these digital solutions.

Kiersten: So absolutely. I think you've talked through, you know, the both the opportunities and the challenges. We know that cybersecurity is an evolving security challenge for the electricity subsector. We certainly appreciate, and particularly at CISA, as we're looking to protect and defend the infrastructure that cyberattacks have the potential to cause severe physical and economic harm. And so the idea is then how do we create that resilient infrastructure? Energy infrastructure has to be particularly important because the energy infrastructure targets of cyberattacks, including by nation-state actors, as well as just global, malicious actors. And when we think about this, you know, hackers can disrupt operations, through ransomware attacks, or by exploiting virtual private networks to gain access to control systems responsible for the critical operational activities. With the electricity subsector operators increasingly integrating industrial “Internet of Things” devices with industrial control systems to help monitor and regulate and manage operating environments, this interconnectedness and the connected devices pose really many of the same risks to enterprise security as just traditional ICS. And in fact, there is almost this exponential connectivity that, you know, as we've seen, both creates opportunities as well as challenges. And so, you know, the inherent risks of these devices include the vulnerabilities in design, manufacturing, implementation, configuration, and disposal. I think one of the key things, as we've talked about is that secure by design, secure by default, as these devices are being created, is so critical. We know that an attack on the electrical power grid could have devastating and cascading consequences. So that is why, you know, when we think about smart grids, you know, what does that actually mean? And I know we're going to talk through this, but I'll just, you know, I'll start with this concept that, you know, a smart grid, you know, according to the United States Energy Department, it's, the smart grid is enabled by new technologies that improve two way communication control systems and computer processing to help the electricity industry better manage energy delivery and transmission. So this, this smart grid approach really improves the ability to analyze the stability of the grid, to identify issues, route power appropriately, provide more information to consumers, and manage and organize all the different segments of electrical generation operation and consumption. So as we look at how do we create this resilience, certainly the development and the investment in smart grids are important. But as you mentioned earlier, Natalia, you know, there's always we have these cost benefits.

Natalia: Yeah, correct, and all the rest I, I have to add, in Europe we see an incremental DDoS attack on 70% you mention as well ransomware attacks, which in general are increasing up to 40%. We also aren't really... let's say, aware of the supplier risks, so a lot of a lot of suppliers are included in our supply chain of the different products that we deliver, so one day afterafter Japan was complaining about the attacks from Russia and the Ukraine, Toyota had to stop the production line and losing 13,000 cars and they stopped not because there was something wrong with them, but they stopped because one of their suppliers had an attack, and in order to avoid that spillover from this attack. So this is adding to the list of risks that Kiersten just mentioned just mentioned in. But nevertheless, I want to to to touch on one topic, because I always get the question whether accessing cloud technologies or using cloud, it's going to increment this kind of risk and actually from the pure cybersecurity perspective, I can tell you it could go different, completely different. So the the the cloud providers, what we call the hyperscalers, they have a really high level of standardization. They don't have, like many of us companies, legacy infrastructure, not updated infrastructure, that could add risk to the equation. And just to give you a really... to give you an example, I was so proud and I am still of the team of Siemens managing the look for vulnerability at the beginning of this year very fast. And now I got told that one of our cloud providers, they manage that 19 times faster than we did. And I consider that we did already that in record time. And the reason of them being able to manage this so quick was because of the level of standardization and the level of standardization that they have, so they can deploy patchess in a matter of minutes. And now I wanted to use this example so that you can you can have, you the audience, can have a better perspective or understanding on why do I say the cloud or the use of cloud is not going to add more risk to to to the equation, to the use of digital... Not, not, not not more risk and not less risk to the use of digital technologies, for for whatever you are using that. Now, given the the political context or the geopolitical context Kiersten... the threat posed by hostile groups and governments... can you talk to us about it? And is the smart grid the perfect target for an attack from the outside? Tell us a little bit more about it.

Kiersten: Well, I think, you know, there are two ways to look at this. I mean, the first is both the value of the smart grid and that this has to represent the future of technology,right? So the smart... the smarter grid should be better equipped to integrate electricity generated by renewable sources such as wind and solar, improving the reliability by efficiently managing and routing power, as I mentioned before, reducing the chance of black blackouts and that all levels of government need to be engaged. So that's that's one way. You're talking about how vulnerable does the smart grid make our energy infrastructure? And this goes to the point that you talk about with cloud, and as well as secure by design, secure by default...this idea that we are creating an infrastructure off of technology, we need that technology based on the limited resources that we have when it comes to energy and electricity. But we have to be baking in that security because any vulnerability, any interconnectedness of this infrastructure to that vulnerability makes it exposed and can be easily exploited or at least exploited more readily. And this is where industry, government engagement and collaboration to build out the security of that infrastructure is so important. And when components like the cloud and others are brought in that there is real attention paid to the security. So when we often delegate the responsibility of functions to the cloud, it doesn't mean that we're delegating responsibility. It doesn't mean that we're delegating accountability, that as an entity, an organization, a company, a government that is using the cloud, we have to hold our partners, our vendors, to high security standards to ensure that they are resilient, that they do have security integrated into that infrastructure. And this is, I think, more and more critical in an understanding of why security needs to be built in from the outset that this is monitoring and control technologies and connected devices become further integrated into the electricity grid in the United States and to our nation's electricity grid, to make it smarter. The grid becomes increasingly vulnerable to cyberthreats that have physical consequences. So building that security into the infrastructure from the beginning is critical, and that will make that infrastructure more resilient to hackers, to adversaries, to nation state efforts.

Natalia: Hmm. Yeah. To add to what you said, something that we do regularly in Siemens as well is to test our security capability. So we have teams of people that are not only doing the traditional testing that probably a lot of you in the audience know, but we also execute the red team means and blue teams, and everything that we have in methodology... from the methodology, that we know to assure that we can attack and look at the infrastructure from the different angles and that we can actually find possible vulnerabilities not only in the components themselves, but in their whole environments... that we put together for ourselves and for our customers and fix those before the attacker can find it. So I, I feel every time very happy to see one of these reports, even if they are in red because they are in threat. I prefer to look at them previous to any other attack and make sure we are going to fix them in advance before they become dangerous. So Kiersten, there was this mentality in the past that isolation or segmentation, that's the way we call it, is or was the best way to protect, and how do you see the awareness, that amount to society that this kind of protection is not only the guarantee to have cybersecurity or the needed cybersecurity. Anything from you to comment on that one?

Kiersten: Are you referencing microsegmentation or the segmentation of of infrastructure?

Natalia: Yeah. Yeah. Correct.

Kiersten: Yeah. I think, you know, there is certainly the the security approaches with micro segmentation and how we look at systems. I think separate and distinct from that is the awareness of the interdependency of our systems. And, you know, in looking at how we integrate devices, how we integrate technologies into infrastructure, the the need to to create that segmentation for security is important. But the recognition also that we're creating increasing interdependencies is an acknowledgment that we have to appreciate.

Natalia: Sure. Now, talking talking from another perspective, I know all these attacks that we see... in that they are increasing... are.... they are are triggering or motivating the different governments to react to this. And you come from an American agency, from that agency of the United States. Can you comment what kind of support, regulations, advice are you providing to to the society from the government perspective?

Kiersten: Well, we're constantly looking at where regulation can play a role. I think, you know, the sequence often is we let market forces do their work, to see if market forces can create incentive. Where market forces can't weigh in or create impact or difference, then bringing in regulation is certainly an option. And I think, you know, we have all of these critical sectors and we have variability around regulation based on where we are in the process. And it's something that we actually this administration, this government today, is actively assessing and deliberating where regulation can play a role. What is interesting is right now, in this time, having worked in this space for so long, you do hear from industry that there is an interest in working with government on developing regulation. I do think whenever there is something that the private sector, that industry has to follow or comply with, that is developed by government, the importance is having industry and government work together. Government can be a convener, government can work with industry, because if industry has to follow in a line, it's only helpful and will create more success and effectiveness if the entities come together to to build that out together.

Natalia: How do you establish that cooperation? Do you have many representatives from the different companies?

Kiersten: It's a great question. So, we have different structures within the United States. So one entity that was just launched last year through CISA, is called the Joint Cyber Defense Collaborative, and this is an industry-government collaboration on sharing threat intelligence data. It's a little bit separate and distinct, but when there are sector-specific threats, we bring in the sector and work together to build that trust. But importantly, since 1998, we've had something called the Information Sharing and Analysis Centers. And those are, the the acronym for that is ISAC, and those are bi-sectors. And those organizations work then collaboratively with government. So over time, what this has led to is the sharing of information within the sector itself so that when there is threat intelligence they share within the sector, but also importantly with government. Similarly, what the Joint Cyber Defense Collaborative has done since it was launched is very much about taking the intelligence and the data that it receives and being able to share that with industry. It's not always a complete and perfect picture. In fact, it rarely ever is, if ever. But the idea here is that we're sharing data, we're sharing data points, so that we can get and build together a more complete threat intelligence picture. We're sharing indicators of compromise and having greater visibility into where the threat acts. We also have an organization called the Analysis and Resiliency Center, which right now focuses on the energy sector in the financial sector. So we see groups that are convened by industry. In some cases they are legislated by government and others, they are just created by industry themselves. And what's important is the communication, the convening, the gathering of these groups with industry and government together. Someone said to me about a year ago when we were talking about industry, government work, that, you know, people don't trust institutions, they trust people. And so what's so important as we're building these out is the development of the relationships with people, with individuals. There are activities and engagements with the organizations that go beyond just the broader institution, but actual individual engagement and the building of trust and cooperation over time.

Natalia: I think you and me, we are a very good example of this kind of person-to-person relationship.

Kiersten: Yeah, exactly.

Natalia: And maybe it's interesting for the audience to know that we at Siemens, we look very, very much at CISA,at the Cybersecurity and Infrastructure Security Agency, they provide us with guidance about which measure to prioritize, about which vulnerability to close. So, we listen very, very carefully to their advice, and and follow their advice. Now, let let me let me take this opportunity as well to to mention that we in Siemens, we as well are convinced that especially in cybersecurity, we need to cooperate,we have to prevent reinventing the wheel, and therefore, we have established with other 16 partners, the Charter of Trust. The brand new partner is Microsoft this day. So we are very happy to have Microsoft in the Charter of Trust, and we have given us ten principles. One of them you mentioned several times today, you mentioned security by the following one, so happy to hear that. And let me tell you, we agree among these 70 partners now, what are the requirements for us in regard to the security by default? So we know exactly which are the 17 settings that we want to preset in all of our products to for this security by default to be and even And in addition to that, we gave us as well the principles in regard to supply chain security. So we also agree on the 16 requirements to be included in all in all of our contracts in the terms and conditions are included. And now we are giving us as well the task to control those providers and to share the results of those controls, those assessments that we will do on the providers so that not everyone needs to redo these assessments. And with that, you can imagine we have partners like Airbus, like IBM, like Mitsubishi, Heavy Industries, like Microsoft now — so the power that we have all together doing and developing this kind of measures together. So, also worth mentioning, and I talk about segmentation Kiersten, and I think there was this mentality in the in the past, and I think this is the best for me... was before COVID, before the pandemic, that we could protect the company by establishing walls like in the medieval times... actually, we call them firewalls and everything what was inside of those walls was trusted, then everything outside was not trusted. And now, with the increase of remote work with the increase of the use of cloud, those walls are there, but they are not protecting the way they should be protecting. And therefore very important for us is the deployment of zero trust. And in zero trust, what we do is to verify that users, machines, devices are secure to access data and we are in the middle of the transformation, and that includes as well the private. The products that we use in the smart infrastructure are going to include this kind of technologies as well, so that the products are able to speak with a policy decision point. This is how we call the device or the functionality in the middle that checks whether the devices are secure to access that. So this is changing the way we do protection and we do cybersecurity in these days. And I am very proud to share with the audience that we are in the middle of it. I promise we will do a podcast only on zero trust. And yeah, I keep looking to the time Kiersten, we are coming to the end. Any final remarks from your side? Anything else that you would like to share with us?

Kiersten: Well, I think as we look at this, as we look at smart grid, as we look at the energy and electricity efforts and infrastructure, the criticality of collaboration and partnership, both between industry and government, but also more broadly... I mean, CISA right now has relationships with over 150 computer emergency response teams, andthis discussion Natalia, with Siemens and the work that you're doing internationally, is so important... with the rapid evolution and expansion of smart technologies and connected devices. The importance of partnership is is so important, is so critical as we move forward and as we look at this problem, it's very much about building resilience. It's very much about how do we create that resilient infrastructure globally with our partners to share the responsibility, to do our part, to build the collective cyber defenses that are truly needed to protect our critical infrastructure now and importantly, to ensure future resilience.

Natalia: Yeah, thank you, Kiersten, for your words, and I would pick on on one point to close and this is the point that that we all need to actively participate in securing our digital world. And you mentioned that, Kierstin, in the past, is [the] responsibility of all of us. We are all and... we are all responsible for the data, for our companies and for our personal data. Four things that I always recommend is register your assets —make sure that your assets and your cloud accounts are registered, similar to the cards. All the technology that was developed to protect the passengers will not work if you don't put your seatbelts on. Similar to that, all the measures, all the technology, all the cybertechnology that we deployed in the companies will not [be of] use if you don't register your assets. If you don't encrypt the information that needs to be encrypted, your emails, your confidential emails, or confidential documents should be encrypted. Please remove as well, your local admin rights. It’s still the case that The most the most of the attacksthey start with the compromise of an administrator account, and in some cases this is the administrator account of a client that was not even administrator, but it happened to have administrator rights. Right. So those single actions and activities will help us to protect the digital world. So think about that and secure Siemens... help us to secure the digital world. So with that, thank you again, Kiersten, always a pleasure talking with you. I hope you enjoyed as much as I did. Thank you very much. And for our audience, thank you for listening and for paying attention to this important topic. Thank you.

Kiersten: Thank you, Natalia.