"When we started to talk about critical infrastructure protection, we started also from this background, providing other institutions a lot of information working together to bring information security forward. And we had to learn that at a certain point, it's a problem for institutions, from the industry to have the resources to make everything, to bring everything in life in this field of IT security. You have always to invest some kind of resources to bring IT security to life."

MARCH 16, 2020

Maintaining Continuity in Critical Infrastructure

Presenter: Isabel Muench

Summary

The amount of critical infrastructure security news has exploded in the past few years due to ongoing digitalization, which has caused an overall increase of dependence on IT. Isabel Muench, Head of Branch Critical Infrastructures at BSI, talks to Brian about weaving IT security into critical infrastructure and shares stories of successes and failures.

Transcript

Brian Contos:

Welcome to the Cybersecurity Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I'm your host, Brian Contos, and we've got a really special guest today. Joining me is Isabel Muench. Welcome to the podcast, Isabel.

Isabel Muench:

Thank you, Brian. I really like to be here.

Brian Contos:

Isabel, where are you right now? Physically, where are you in the world?

Isabel Muench:

I'm physically in Germany, in Bonn, the former capital of Germany.

Brian Contos:

Wonderful, wonderful. Well, thank you so much for dialing in for this. Before we get going, and we have a number of questions I'd like to go through with you, but give our listeners a little bit of background about you and the path you took that led you into cyber and what it is that you do today.

Isabel Muench:

Yeah. What I'm doing today is I am the Head of the Branch Critical Infrastructures within the BSI, the German BSI, which is the German Federal Office for Information Security.

Isabel Muench:

I started with the BSI some time ago now. First, I started math and computer science. And after my diploma, I was thinking about what can I do now with a lot of math. I wanted not to continue with really core math like I studied because that had meant to go into cryptography. And as you can hear, I nearly can't pronounce "cryptography," when it's in English. So, I started as a consultant, as an IT security consultant to be precise. And that was one of the best choices in my life because IT security or information security as we say nowadays was very good and proud field and it is always developing, and every day you have some new challenges and every day something which is really new to you and it's never boring.

Brian Contos:

Yeah, well, absolutely. And you picked an area within I think information security that's probably one of the hottest topics right now. And that's, you work a lot with critical infrastructure. How do you define, and I'm going to ask this question because I hear it's defined in so many different ways, but how do you define critical infrastructure and why do you think it is such a hot topic right now globally in information security?

Isabel Muench:

We have an official definition of critical infrastructures in Germany that says critical infrastructures are organizational and physical structures and facility of such wonderful importance to a nation, society, and economy. That their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other traumatic consequences.

Isabel Muench:

As far as I know, it's nearly the same definition as the US or Great Britain are using for the definition of critical infrastructures. And you can say it in short, critical infrastructures is everything which is really important to you. Like

energy supply, like health supply, like finances, everything which is really important and would really matter if it's not existing anymore.

Brian Contos:

Yeah, and I think a few years ago, and I don't know how many years you go back, but intuitively a lot of people thought of critical infrastructure as power and energy, oil and gas, transportation. But I think you make a great point that it's the financial infrastructure, right? It's healthcare. It's so many of these things that really impact our daily lives, and I think that's true regardless of the country.

Brian Contos:

Why do you think it's been taking center stage in the news? Critical infrastructure has always been a topic. I don't want to say it hasn't been, but as of late and as of late being the last few years, it seems like it's always being spoken about at the conferences. There's a lot of articles and blogs about critical infrastructure security that's on the news. Why now? Why have we just started to really take notice, do you think?

Isabel Muench:

Because of the ongoing digitalization we are more and more dependent on IT. And if you are dependent on IT, you have a totally different view on critical infrastructure protection because we are distinguishing the normal protection of critical infrastructures, what you can do physically, like extra transport line or things like this. And critical infrastructure of information, critical information infrastructure protection, or in short, CIIP, with double "i" in the middle, and this developed really quick in the last 10 years.

Isabel Muench:

When we started, we had to explain to people for example, from the power sector, from the health sector, for example, how dependent they are [on] IT nowadays. When I'm looking around in the last year, now everyone knows that they are dependent [on] IT, and so they have understood that it's a really important thing to care about. But it's not easy, there is a lot to do yet to have a good level of critical infrastructure security.

Brian Contos:

Yeah. You know, I don't think I've ever had a discussion with anybody in critical infrastructure that doesn't sort of append the conversation by saying, “And there's still a lot to do.” I think there's a lot to do in any area of information security, but certainly critical infrastructure.

Brian Contos:

Being that you have a high level of expertise in here, I'm always curious when you first got involved on the information security side of critical infrastructure, what were maybe some of the things that surprise you today?

Isabel Muench:

There are a lot of things which surprise you every day, but what one thing which is surprising nearly every week is that when we started, we provided services. We defined ourselves as a service authority, something which sounds sometimes funny for people from outside because we provide a lot of free information to everyone in the world.

Isabel Muench:

A lot of our information for sure is in German because we are situated in Germany, but we provide also a lot of free information in English and other languages. If you want to have a good laugh, you can look up for example, one of our key documents which is translated in Estonian. Estonian sounds very funny. And so, we provide a lot of information and services for free and so we called ourselves something like a service provider. We make consultancy in Germany and for other authorities, it's also free. We have a lot of services which we can provide for free and especially a lot of information which we provide free.

Isabel Muench:

And when we started to talk about critical infrastructure protection, we started also from this background, providing other institutions a lot of information working together to bring information security forward. And we had to learn that at a certain point, it's a problem for institutions, from the industry to have the resources to make everything, to bring everything in life in this field of IT security. Because what you also have to learn IT security is always... You have

always to invest some kind of resources to bring IT security into life. We can make a lot of things roundabout the information security to make it easier to be used, but it will never be without any problem to use. You have also always some resource that it will need and within the industry it's in the most fields, it's not the key business thing, which they are doing in the industry.

Isabel Muench:

It's not that they start a new service and say, “Oh, this service is about IT security.” No, normally the service is about healthcare or power supply or whatever, and it has to be secure but it shouldn't need too [many] resources. And so, we have to think about how can we bring more IT security into all these different kinds of industries. And after some years of discussion, our politicians, like politicians in other countries also decided to make this the law. And in Germany, we have now the German IT Security Act, which is similar to the European NIS Directive. NIS for network and information security and which tells companies from the critical infrastructure what they have to do about information, about handling IT security incidents and which kind of safeguards they have to use and to set up to make their critical infrastructure areas really secure. So, a lot of things they have to do.

Brian Contos:

Yeah, a lot of things. And it sounds like you've put together, and your group has put together so many great resources as well for people. I'm wondering, from your perspective, do government organizations and industry that operate within the spectrum of critical infrastructure, the higher ups, the leaders, the executives, do they understand some of the risks that are associated with critical infrastructure from a cyber perspective or is there still a gap?

Isabel Muench:

The gap gets smaller every day, I think. Most of them understand that they have to do a lot for the protection of their own critical infrastructures, but on the other side it's not cheap and it's not the main point of their business. That's the problem normally. And a problem we often have in companies from the critical infrastructures is that the people who are within the companies are concerned with critical infrastructures and their protection are too far away from the management and sometimes we have something like a translation problem. The people from the IT, the people which are responsible for IT security of the critical infrastructures, normally called CISO or something like this, they do really have to know what to do for the protection of the critical infrastructures. But sometimes they have the problem to bring this on the table at the board. And for this, we have learned it was a good thing that we in Germany now have a law which helps the people in the companies responsible for information security to bring it on the board and on the horizon of the business leaders.

Brian Contos:

Now, I think that's, that's very refreshing to hear, actually, because if I think I would have asked you that question just a few years back because I've heard the response from many people in the space, it's that they just don't get it. There has to have been a lot of evangelism and education and awareness and I think by and large thanks to people like yourself that have moved them forward, if you will. I'm wondering, could you share some stories with us about maybe some things that have gone wrong as well as some things that have gone right in terms of that intersection of cyber and critical infrastructure?

Isabel Muench:

Yes. Stories about what went wrong, you can find almost every day in the media. You always find the same kind of stories, DDoS attacks here, or passwords published there, or 400,000 user entries opened to the public within other company. You just have to look up what you can, just what you can find every day in the press. And I haven't checked it for today, but I'm really sure that also today, we will have some thousand, 10,000, or sometimes 100,000 and more incidentally opened data to the world. Stories like this, we can really find every day.

Isabel Muench:

In Germany, we just had a story where something that started wrong, which had been an attack, which was successful, now a good solution. As you will know, you will have, in a normal open network, IT network, you will have every day new attacks. And you can't do anything against it, but you must be aware that there can be new attack every day and that you must have your ... All staff must be trained to deal with attacks, especially if they will be a little bit successful. And within the healthcare system, it's especially a problem that business is concentrated on healthcare, not about IT security.

Isabel Muench:

And we had a group of hospitals in Germany which had started in July, from our point of view, a typical ransomware attack, which had been successful. And what I didn't do was to look at their ransomware attack and say, “Oh God, oh no, we can't do anything about it.” What I did was, they had a business continuity plan for this kind of incidents. They used the incident response plan and called us for help as well as other institution which could provide some help so they don't started to panic. They started to act. They acted in the right way. We had a lot of very good talks with them and we exchanged a lot of data and found where the entry point was for this kind of attack and could help them to get over it. And this helped us together to remedy the situation and also was possible to analyze what happened and what is most important. With this kind of incidents, we were able to contain the incident.

Isabel Muench:

We expected the first try to re-install a fresh and remedied system, ended up with re-infection of this ransomware. But through analyzing what happened and where the entry points was, we were able to gather the very good IT team of the hospitals to finally contain the incident and set up the IT systems which were affected and so that they were able to get back to normal work very quick.

Isabel Muench:

What was really good for us was that it was so quick. Quick means from the detecting of the incident to finally going up into normal stage again, it took us some days. But it was on the other side so quick that the patients of this hospital did not notice the incidents. But from the press, from some time on, we had to tell the press what happens because some minor systems where this was be viewable from outside that they were affected. But the hospitals, with their healthcare systems, were able to work all the time.

Isabel Muench:

And so, this was for us a great success story where you can see what a good business continuity plan in the beginning, how this is a good starting point to handle an incident. Not to go into panic, but to react on a proven and good way. And the other thing we learned here again is how good networking helps you so that you can analyze the situations in a quick way. And so this was for us a really good example when the thing which was not so fine, ransomware attack is always a lot of trouble, which worked out very good.

Brian Contos:

Yeah, and I'm glad, Isabel, how you tied that in with business continuity because I think that's a ... If ever they are required continuity, it's within critical infrastructure. I like that picture you painted so thank you so much for that. Isabel, there's a question we'd like to ask everybody that's on our show and it's kind of a fun question, if you will. And that's who's your favorite superhero or supervillain and why?

Isabel Muench:

Yes, my superheroes are Donald Duck and Uncle Scrooge. Well, as I know, it's called Scrooge McDuck in English. As I have learned, Donald Duck and Scrooge McDuck are more famous in Germany or in Europe at all as in US. Donald for me, is a really good example for the duck from next door who is facing new challenges every day, who is handling these challenges, who fails also regularly but always is able to manage and to master the challenges together with his family and his friends. You will never remember stories about Donald Duck or the family from Duckburg, when something is really going bad. Normally, every story has a good end. And if you are looking at classic stories, it has to do a lot with the protection of critical infrastructures, especially if you look at Uncle Scrooge.

Isabel Muench:

Uncle Scrooge's daily business is to protect his critical infrastructures, his money bin against the Beagle Boys in the classic stories. There's a typically physical attack. They are building tunnels under the money bin, they are flying attacks, they are bombing the money bin or whatever you can think about. And nowadays, in recent stories, also digitalization has found its way into Duckburg and you can find the Beagle Boys on the internet trying to attack the money bin, the virtual or money bin via the internet. That's not only funny, you can also learn a lot about the daily life in Duckburg and you can also use it for explaining people about information security and it helps a lot if you are explaining them more or less complicated than the things you have to tell users about information security when you can use the funny pictures from Duckburg.

Brian Contos:

Yeah. Oh, I love it. I love it. I love the evolution of the Beagle Boys from physical to digital. Great. That was a fantastic example and I don't think I'll ever look at Donald Duck the same way now, so thank you for that, Isabel.

Brian Contos:

All right. Thanks to all our listeners for joining and be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.