Interview Jacoba Sieders – TrustTalk podcast

Voice-Over: Welcome to TrustTalk. Our guest today is Jacoba Sieders. She is one of Europe's leading experts on digital identity. She talks about what it takes to get cybersecurity through identity, access management and the security concept of Zero Trust, the belief that organizations should not automatically trust anything inside or outside their perimeter and instead must verify anything trying to connect with systems, before granting access. Identity is more than just a person. It can be a "thing". It is all about the data of users, businesses and organizations. She reflects on the tensions between digital security and privacy, on dynamic access validation and trust of anything trying to access data. She is critical about the level of risk awareness in government and the lack of risk monitoring. Your host today, Severin de Wit.

Interviewer: Jacoba, you are a specialist in digital identity and what is called Identity and Access Management, or IAM. In this area you have a very broad background, you worked for various large financial institutions, like a Dutch headquartered bank and the European Investment Bank. And at the moment, you are a consultant. So what are the current trends in IAM and data protection?

Jacoba Sieders: The current trends that have been going on for a long time already in data protection and data storage and data security, that digital services are crossing value change of services. So it's not one set of data compiled in one safe and secure castle for a company, for instance, and you can lock the front door and that's it. No, data is constantly in transit across multitudes of devices and people and services. So there's a lot of multitude of shares and distributions of the data. So it's like sand everywhere and everywhere in small compartments that all need to be secure instead of securing one big castle like we used to do. And also, users are far more aware about their data privacy because the GDPR, the General Data Protection Regulation, from the European Union has had a lot of tension. So this is a different world than the world we used to see and we need to protect it in a different way.

Interviewer: Yeah, today we are talking about Zero Trust, digital identity and security. And when we prepared for this interview to set the scope of our conversation, we agreed that self sovereign identity or SSI and the legal challenges surrounding it should be part of the interview as well. However, as there are so many aspects to be covered today, we agreed that we would focus on SSI and especially the legal implications in a later podcast in the autumn of 2021 and today focus on the aspects around Zero Trust and identity and access management So my question comes, it's in your area of expertise, I seem to discover a lot of acronyms and terms that sound unfamiliar, like zero trust "least privilege" and "application control", SSI, IPI. Can you shed some light for the uninformed how these relate and what is the common denominator?

Jacoba Sieders: Yeah, they all relate to the protection of data and the right and not to0 wide access to a set of data, only the person who needs to see it, can see it, as long as he needs to see it, and only for the time that he needs it. And we would not let people access more data than they really needed for the job or the transaction that is required at the moment. And I think it's good to go back to the traditional setup of identity and access management as we all knew it and know it. And then we could move on to the Zero Trust way of doing things in a yeah, adaptive way. Adapted to the current data storage and data usage trends, as we just described them in the previous question.

Interviewer: To understand what AIM and digital identity is let's go back for a moment to my younger years (I have to say that's some time ago) OK, imagine myself, I want to go out on a Saturday night having a good time. And a famous club at a time was where we decided to go to with some friends. And we knew we had to stand in line for this popular club, we knew it would take a while. And there he is, the first hurdle. A tall, broad-shouldered Doorman. He looked carefully at our ID and checked if it is not a fake. And every time he turned his eyes, he made a calculated, very individual assessment on whether I and my friends looked like someone who would be safe to let in and can be trusted. I'm pretty sure he made all sorts of judgments like, how is he dressed? Who are his friends joining him? Is he clean? How old is he? Is he under influence and does he look familiar, reliable, etc.? Wouldn't you say that was our Doorman did was Identity and Access Management avant-la-lettre?

Jacoba Sieders: I think so, yes, it certainly is. It's a very, very good comparison between what we do in the digital atmosphere. There's a Doorman who decides who to let in and who not to let in, and he makes judgments to check your identity. If we translate that to digital equivalent, we see that there are three main parts at stake. First of all, who are you? Are you, your identity and secondly, are you a member of the club? Do you have entitlement or "authorization", as we call it, in the identity world. Authorization or entitlement to enter. Are you a member of this club? Are you on the list of people who have the right to enter and then the "authentication", that's the way of proving that you are you and the Doorman could have asked you a ticket or a passport with your photo ID or a password that you needed to mention. So you prove that, yes, I am that person that I claim to be. So the identity, the way of showing that really you own that identity, it's you. And the other thing, the authorization or entitlement, that is you are a member of the club and you paid, and yes, you are one of those people who are entitled to enter.

Jacoba Sieders: Those three elements, Identity, Authorization and Authentication, this happy threesome and you need all three of them in identity and access management. And identity could be less important, but access is important. And most users, they don't need their digital identity. They just want

to enter somewhere. They want to do a transaction online. And that you are requesting as a company their whole identity and a lot of attributes to judge them, that's not in their own personal interest. And this is where the challenges are in traditional identity and access management.

Interviewer: Let's take a step back. Zero trust. What is it and how does it relate to identity access management and security?

Jacoba Sieders: As we refer to in the beginning of our conversation, data used to be safe and secure within a company, within a parameter and we could trust that if the data is in our own servers where we as a company are working with, and where we have our boundaries and our parameter safe, we could trust data in there and we could trust the devices and the users inside because we've all checked them. Today, when data is all the time in transit, is connected to a lot of partners across the network, outside of our own company, people are working from home and people access data from a lot of types of devices and this big distribution of data in transit is everywhere. We have Zero Trust. And Zero Trust, this is the way, it's what stands for the protection of data in this type of setting. How can we make sure that the data is still safe and secure, although we have zero trust in the location or devices or environment where that data is residing or where it's used to. So no matter the location, even inside, we don't trust anything. So we need new types of protection, new types of architecture and access management to make sure that still we can work safely.

Interviewer: So let me see if I understand. If we talk about digital ID, that would include what we have in the Netherlands called DigiD, but also could be a profile I made or a code or my even my Google mail address.

Jacoba Sieders: Yes, correct. I always say that digital identity is a digital reflection or a digital representation of a human user. And that's a bit old because today we even have digital identities of your car. It also has an ID. It's also a user and a thing, a camera or anything could have a digital identity, a digital user ID,

Interviewer: Even my freezer.

Jacoba Sieders: Yes, that would be the identity of thing, as I call it, the Internet of Things. So if we talk about this network like we just did all these things and devices and cars and people and human and non-human are interacting with each other and for instance, even a process or a transaction could have a one off ID. It travels through the network and through the data and it's a process, but also that could have, like we used to have, session IDs and networking. It could have the need for an ID. So it's a digital

representation of an actor. And in the old times, we mainly mean human actors, you and me, when we talk about digital identity, DigiD or any ID in an eco system that would be a human actor, but today we talk about actors that could also be things or processes or whatever.

Interviewer: Currently the subject of digital identity seems very much an incident driven subject. Attention to digital identity and security pop up only when things go wrong, it seems. When someone with a stolen identity commits a fraud, or does things in my name where I did not authorize it. So how should AIM and identity be looked at to make sure that organizations put more effort in it?

Jacoba Sieders: Well, that's an interesting question and an important one. Identity management or access management is one of the preventative controls. When we want to make the world more secure, we prevent intruders to enter. So it's the front door, as you said, like the Doorman. It's a very important part of the security of my assets. And what is always going wrong is that it's seen as being an IT thing. It's this stupid security department in IT, I lost my password, I have to reset it, it's bothering me, I don't like it, but it's an IT problem. But if we really look at it, we know that it's really the data that's owned by users or by the business. It's their data, it's their intellectual property. It's the privacy of their customers. It's the privacy of citizens. And so it's a real huge business interest to keep it secure and therefore business attention on the top level, in the really Board level awareness, about the importance of digital security, should be available. And if we have at least one person in the Board or one person in Management who knows why this is important, and who can help to gain budget for that, that's one way of doing it. And then for the implementation, often security is seen as a sort of plaster that you stick on, you know, you make a nice app, you make a nice application and then, "oh yeah, security". OK, yeah, password. Stick a sticker on it, so now it's secure. But really from the architecture and the design, really from the bottom fundaments, it should be thought with Zero Trust in mind, with thought that nothing is secure and you need to build your architecture from the bottom up with the security mindset. And that's important. And it's also very expensive. And security professionals are scarce and it's often an expensive part of the IT budget. But if you don't do that, if you would it half, I mean, one leak and everything is useless. Half security is the same as zero security.

Interviewer: You mentioned the word "digital representation". If we assume that in an average sized bank, employees are working with approximately 3,000 applications ranging from pure financial apps to community communication apps, and each of those has its own method of allowing a party to access. That's what we call digital representation, isn't it?

Jacoba Sieders: Well, I use it more in the human atmosphere, like it's you are being represented with all your attributes, the properties you as a person have like the Doorman, are you drunk? Are you a lone

customer that has been here for 20 years with a good if we talk bank, for instance, did you always pay your bills properly? You can have different ratings as a customer or different ratings for trust, can you be trusted as a customer? So that's a digital representation of a digital identity. That's what I meant with it. But you are rightly stating that a bank has 3,000 applications and when you go back to the Zero Trust atmosphere, in order to decide what a customer could do or couldn't do or could pay or what transactions and how to validate that, this is really your digital representation of that human person who is now at my doorstep digitally. We want to make a very dynamic decisions on what a customer could do. We don't want to have all the zillions of security measures at the front door when the customer is only doing a very small transaction, that's low risk. And we want to step up that level of preventative controls at the front, maybe with extra checks and extra logins or more trust checks when there is a large transaction at stake. And there are certain methods, we call them "Attribute-Based Access Management". We check a number of we validate a number of data points, and if that data points can be rule-based, we can check and then we could decide that in this case, this is a transaction you're doing every day. It's not a huge amount of money. If you always go to this bank account to bring them their money and it's always 14 euro, you'll always buy that same dressing at Zalando or whatever, online, OK, then this is such a regular pattern for you as a customer, we can trust it because pattern recognition helps also for finding the places where it's not trusted. So if we talk zero trust dynamic access validation and not a stable fixed set of things that you could or couldn't do, but dynamic, according to the risk level attached to it, we could decide yes or no or, to a certain degree, how secure it has to be. And that concept can be brought on, to all, for instance, employees, when they work with 3,000 applications and all these applications know things about the employees or know things about the pattern they day use, and if you use that data for making risk decisions, it means that although it's still unsafe everywhere and nothing can be trusted, but you can have a lot of information or probability that, yes, this will be this person, and yes, it's right, like the Doorman when he looks at you, that you're probably not drunk or probably drunk. This is all data attributes helping for the decision.

Interviewer: Digital identity and security seem to be not, you cannot discuss it without taking privacy in the equation. So is there a trade off between individual and group privacy and the concept of digital security?

Jacoba Sieders: Well, I always call privacy, security and usability, which is an important one. That's really a triangle. The more usable, the easier the access is, to certain system, or door, even your own front door, the more usable, the more easy it is, probably the less secure it could be. And the more private you keep something, yeah, the less secure it could be. So if if you are giving me a lot of information about yourself, next time when I need to recognize you, the more data I know about you, the more secure, the more safely I can assume that, yes, this is you, because I have seen your face, I know your

voice, I'm sure it's you. If you keep your mask, if you keep your face masked, I can't be sure it's you, so security is lost, but privacy is gained. And usability, privacy and security, you all want them, all three of them. But in practice you're always violating the one when you improve the other. And security, when we talk about group security, then we talk actually more about surveillance. If we have these safety cameras and we check a lot, it means people are less private. So, yeah, there's a tradeoff indeed, as you state between the three of them.

Interviewer: Is there a single identity to get access to all kinds of services? Is that the cure, maybe? Like one ID for me paying my tax, gets the governmental departments, get access to my bank or get myself registered at websites, location services, subsidies, get a mortgage, assets and so on and so on. Would that be the cure?

Jacoba Sieders: Well, in a way, it would be, of course, a cure for your usability. And here we are again, the safety and security would be less high if that's one identity was caught. You would have as a fraudster, you would have access to all those services that you just mentioned. So this is an illustration of less usability is more security, and vice versa. Now, we have done some interviews with the Dutch Payment Association, interviewing users of banking services. And one of the outcomes was we asked them the same question, would you like one identity to do all, to make life easier? And it appeared that most of those users would say, well, I do have three different email addresses, one is my real one, when I do serious business, one is a fake one or a dummy name for whatever, so if I expect there will be a lot of spam from a service that I subscribe to just from a one-off service, and then I have one other one, which I rarely use for really going to untrusted services. So in practice, regular users who are not specialists, they use three different identities for three different or mail addresses then, for three different levels of security. And I think that's a good idea. When we talk about Self Sovereign Identity, that's a completely different concept where you have a wallet with identities in it and you use the ones you need for every case separately, but from one point, that's a different concept. I can't discuss it here, but that would be a very nice.

Interviewer: No we are going to do it in the autumn, right?

Jacoba Sieders: Yeah. So I cannot discuss it here, but that would be a real good solution in my opinion. But I think one single solution is less secure when it's unless you create a very safe way of doing it. If we look at, for instance, Estonia, they had you can be an "e-Estonian", wherever you live in Europe, you can register as e-Estonia, an Estonian citizen. Estonian citizens were not used to have passports like we do, but an identity card with a chip on it. And I think way back in 2013 even or 14 maybe I used to talk to the guy who was implementing that they had an Estonian identity that was really expanding for driving

license and for a lot of those services like you are mentioning them. And this card with that chip would be your one identity to do a number of these things. And today in The Netherlands, I think it's a trend which is also happening, that one identity is trusted in multiple areas, for multiple services. I read that banks are trying to make your identity, your bank identity, being used for the for the tax registration, like IDIN, you have a bank account that could be used for the tax registration. That's since, I think, 2017 that emerged for the first time or for travelling by train. So I think that's a trend that is certainly moving. But these remain different ecosystems and it will never be one for all. That means that all these parties to would have to trust each other's identity.

Interviewer: You mentioned Estonia. Let's have another look abroad. In the UK, there has been talk that there is no need for a national identity scheme, but they would rather think of a national entitlement scheme. So if I want access to a government service, for example, I'm entitled to that and I'm entitled to get into a bank detail. Or let's give a more timely example. If I'm vaccinated against corona and I want access to a certain place or event, I need entitlement to do so, without giving away my identity. Because that would only give away another opportunity to breach or compromise my identity. What do you think of that?

Jacoba Sieders: It's interesting when you discuss the UK, I remember that I was at the University of Leuven in 2012 or something, and I heard somebody from the UK talk about the UK National Digital Identity Scheme and how they never, never, ever were able to set that up. So and as you know, when you want to be residing in the UK, your address and your proof of address is valid as a way of proving that you are British. Of course, you also have a passport, but they don't have one physical, like we have the "Burgerservicenummer", the civil number of every citizen. It doesn't exist in the same way in the UK as we have it. And when you don't have that, it's also very difficult to create a digital version of that. If you want to prove and that's now going on with the UK when we have Brexit, British citizens abroad or any British citizens, they have to prove that they want to register and be a Brit and they can't go to this big registration of civil numbers, so you have to bring your passport or your driving license and a whole list of different papers you could bring or proof from your employer, your address, your passport and a referee, somebody who could judge that "yes, you are you", and "yes, you are living here for a long time". And they have a very complex set of types of proofs and checks and balances that the citizen could use. So yes, yes, I want to be Brit, I am a Brit and I have lived here, I want to belong. So this is really a big problem in the UK. So I imagine that, yes, they have a nice way of saying that it's an entitlement scheme, but they never. Yeah, it's in my opinion, my impression is that they never managed to get the identity scheme like,

Interviewer: Oh, let's forget about that one then.

Jacoba Sieders: It's not there

Interviewer: let's forget about it. So maybe we can focus again on an industry where you worked for quite some time, the financial sector. And especially the role of the European Directives, especially the Payment Services Directive II or PSD2, as it is called. So what does it do for identity and security in financial transactions within Europe?

Jacoba Sieders: Yes, a lot. Well, the idea for setting up Payment Services Directive II, the Directive I was setting up the single European payment area. So within Europe we could all easily make payments across Europe. That was the number one Payment Service Directive, and then number II, it expands on that. It the idea was that there are banks and they sit on a lot of customer data and they know all these transactions. And that's a big wealth, big value to have all this data. And there are payment service providers, and today we have about seven hundred of them. Think about paying PayPal and all the other, Adyen, those they provide payments, that's their service, but they're not really like banks. And there should be more equality between the two types of financial institutions, the Payment Service Providers, they should also have a right to get to the data and to use the trust and data that banks have gathered to make the world more equal. Make more, now, so the idea was that if we let these payment service providers access the same data that these banks own and possess and gather, they could also have some good use. They could benefit from that. So the Payment Services Directive II prescribes that every regular bank, account service provider, with a real bank account, should open up their back office, so a Payment Service Provider could access the customer's data, the transaction data of customers, if the customers give consent and if there is a strong customer authentication, it has to be secure back door. So the Payment Service Provider could use that data and leverage on that or find new business models. And then there are two types of three types of services. The one is that accessing the customer's data and a second one is also originating a real payment within the bank, done by PayPal, and the third one is confirming that a customer really has enough funds, when we talk about credit cards. That there is that it's backed by a bank account that has enough funds, these three services. Now, of course, it means that we are as a bank, you are keeping the front door very safe and your audited three , twice per year and really, really strict, strict, strict evidence, blah, blah, but a payment service provider can go through the back door and get that data or look at that data and what happens with that data when it's there, with PayPal? I can't secure it any longer.

Interviewer: Jacoba, we have only a small time window. So I want to ask you a couple of more questions. And we have to unfortunately conclude. Let's turn for a moment to cybersecurity, because I think you said that it consists of three elements. confidentiality, availability and integrity. Well, take

confidentiality. Again and again, we are confronted with security failures. That is seriously eroding trust. Personal data in databases that are being breached, the recent development in The Netherlands with the regional health organization, GGD, that's the Dutch health organization, personal data where rather easy to access and even be sold to third parties. So on all these three aspects we just mentioned, the system seems to fail. What does it tell you?

Jacoba Sieders: Yes, well, coming from a banking background where I'm used to a lot of governance, control, audits, risk frameworks, management of risk, really almost too heavy for some and very expensive, it's a very expensive business. I'm not aware how the governance in government is being done, but if they would have to set up the governance, so the management, if they were more aware and if that would be more audited like we do within banks, maybe not even that heavily, this could prevent a lot of this. But obviously, and this is not my knowledge, but my estimation, the level of risk awareness in government and the risk monitoring and risk management is probably failing a lot. And the awareness and governance also, it's probably not so well done. And it's not about preventative control only, safety and security in the IT and the log-in and log-on and that type of stuff, but expect also detective controls too. If something goes wrong, do you notice that? Is it found out and what do you do? Those are two parts preventative and detective controls and risk management. I think they are probably not mature enough. That's my estimation.

Interviewer: A last question relates to security legislation, the law tries to catch and solve all aspects of security. When we talked about this in preparation of the interview, I liked your comparison with the Dutch dikes. One third of the Dutch dikes are below sea level, right, and in 1953, the dikes broke, resulting in a major flooding. And so how do you see that comparison of the Dutch dikes relay to drafting security legislation? Explain.

Jacoba Sieders: Yes, I use that because my statement is that you can't measure security. And something that you can't measure, you can't prescribe the protection levels of something you can't measure. And in a dike, you can measure in centimetres how high it should be, how wide it should be. You know exactly it's water and it comes from this end, and there could be some storm and there could be some other impacts. But you could measure everything and then prescribe what type of security you want. But in digital security you never know where the risk is. You never know where the attackers are. You can't measure the risk. You can't measure the security. You can only estimate the risk. But the moment you have measured or estimated the impact and the chance that something happens, the risk level, and that is chance for impact, it's already changed, because the attackers change every day and gets wiser. So, and if you make a law prescribing the relevant security level, you can't write down a technical statement that you should use this technology and this technology and then it's safe. Because it's first of

all, it's already outdated as soon as the law has been accepted. And thirdly, you could never describe all the measures that would be needed. You can only, and a law should be a generic thing, that's a lot of measures should fit into that legislation. So that's my the problem with these laws. You can't be technical and very precise, but if you are not precise enough, you get a lot of problems with interpreting what would be this right level of protection. So you always got a lot of standards and they have to be discussed a lot, and I think that's a very difficult thing about security. It can't be measured. Only risk can be estimated.

Interviewer: There seems to be a lot of subjects that we still have to cover and hopefully we can do that in our podcast in the autumn of this year, among which are more legislative issues, as we said in the beginning, on SSI, but also the EU regulation on Electronic Identification and Trust Services. It's called eIDAS, right?

Jacoba Sieders: eIDAS, yes.

Interviewer: That seems to me like a subject we have to keep because we are running out of time. Well, Jacoba, thank you very much. Obviously, there is a lot more to say. You have enlightened us a lot about the subject, but hopefully we can talk to you again in autumn on these remaining subjects. Thanks for being available at TrustTalk for the moment and hope to see you soon.

Jacoba Sieders: Yes, thanks for having me. Was my pleasure.

Voice-Over: We hope you enjoyed this episode of TrustTalk. We would be very grateful if you leave us a review on Apple Podcasts or on Stitcher. Don't miss out on future travels around TrustTalk and subscribe to this channel or visit us on our website TrustTalk.co or on Twitter at TrustTalkCo. We look forward to seeing you again.