The Future of ERP EP7: Securing Data and Applications in the Cloud & How This is an Opportunity for Cybersecurity with Accenture and SAP

Gabriele: The future of ERP resides in being the human best friend. So what I mean by that? The ERP will run besides us. It will learn from us and it will help us doing many tasks of our daily job. Those are all the tasks that we never get to do on schedule simply because we just don't have the time anymore. And this is true of course in my security area, but it's in pretty much every area of the business because we are just too busy in our lives nowadays.

Richard: Welcome to the future of ERP podcast. My name's Richard Howells. I'm the Vice President for thought Leadership for SAP's ERP Finance and Supply Chain Solutions, and I'm joined by my co-host Oyku.

Oyku: Hello everyone. My name is Oyku Ilgar. I'm a blogger, marketer and podcaster in the area of ERP and supply chain at SAP. And today we are going to discuss securing data and applications in the cloud and how this is an opportunity for cybersecurity with our guests, Andreas Kirchebner from Accenture, and Gabriel Fiata from SAP. Welcome gentlemen, would you like to introduce yourself please?

Gabriele: Hi everybody, my name is Gabrielle Fiata and I look after the cybersecurity market strategy at SAP.

Andreas: Hello everyone. Also from my side, my name is Kircherbner. May my introduction will be a little bit longer. I've been with Accenture since now one and a half years as sub security lead in Austria. And recently I took over the role as global main contact for sub cloud security and sub partnering. But before I joined the consulting world, I was for about 13 years on client site at Swarovski, where I started my professional SAP career as a base administrator. And after nine years I started to focus purely on SAP security. And, there I had the chance and I was given the responsibility for a secure configuration and operation and the proper security management for the entire SAP environment, which was really a very huge task, but it was really amazing. And also when I started to focus on SAP security, I also found a new passion. And so I started to

contribute to the German speaking user group, the DSHG. And there I was also elect the spokesman of the SAP Cloud Security working group in 2019.

Richard: Okay. Thank you both. We've certainly got the right people on the call to have this discussion. So let's start with a basic question , what does it mean to secure a data in the cloud, and how is this different to on-premise deployments? What's changed?

Gabriele: Yeah, so I can take that Richard to start. So cybersecurity, it's now one of the top strategic business objectives. So pretty much every company, if we look at the World Economic Forum earlier this year, there is a raising concern on business application security and also security when it comes to public infrastructures.

Gabriele: If those are breached processes could be stopped for days and months and sometimes that could have a critical impact on communities, but also on businesses. Also, data could end up being sold in the dark web and organizations and companies could have to pay sometimes costly fines. Sometimes they will have to pay ransom, and here we're talking about millions of dollars in some cases. Now what's new in the cloud? The cloud changes the threat landscape for those organizations and companies. Previously, they had to manage security within the four walls of their organization, primarily leveraging their internal security teams, which were running the security operations. Now as data and applications are running in multiple locations in the cloud and they're always available and accessible simply through web browsers or mobile apps. Now companies need to rely not only on their internal security people, processes and technologies, but also on the ones from the cloud ERP providers.

Oyku: Andreas?

Andreas: Yeah, so not only the Strat landscape has completely changed as Gabriel has already mentioned the way how we need to deal with our environment has changed or is changing now the classical parameter security where we've trusted our environment within our four walls, where we clearly knew what happens and what's going on. This is now opened to the outside of our environment. And so with the move to the cloud, zero trust is getting more and more important cause of the highly interconnected systems with different levels of security. And many of these systems are outside our control where we can no longer be sure that the end-to-end architecture is secure. So we also need to consider the different deployment models, what we have and the related change in the responsibilities. When we have a look in the past, SAP security was small or less always in the responsibility of the basis team. So the roots of

the SAP security topics are more related to secure configuration of a system. But with the cloud environment, the client is less responsible for the configuration part, and he needs to have a closer look at all the compliance topics, and maybe this sounds easy, but in reality, the necessary skill set is changing ality. And here it's also getting very tricky because in many cases the BASIS team is still responsible for the systems. But the classical basis administrator needs now to deal with all this information security frameworks, the different contracts, legal stuff, technical, operational, measures. And probably he's not interested in it or does not have the necessary know-how. And on the other side, we also need to notice that basis administrator might has already been imposed to a burden, the inner conflict of the decision what is more important? Shall I switch on a bare meter because of security reasons, which might lead to a system outage? Shall I switch it on or shall just avoid to ensure a stable system operation and not being punished or ordered for report to our business leaders. And we all know that the business partner can become very uncomfortable in case of an issue and, if we are no longer able to sell our stuff. Then, yeah, it'll not be a lot of fun for the business admin. So probably security draws the short stick at the end. And to sum it up with the huge amount of different security topics, security can't be done beside the daily work. And so we should maybe also rethink the concept of the security responsible. And, they can only care about SAP security topics and connect all the dots and try to get away from the basis stuff.

Oyku: Can we talk a little bit about the main concerns that companies can have moving their ERP to cloud from a security perspective?

Gabriele: If we think about it, the data stored in the cloud is accessible from anywhere. It's always available, and it can be easily shared with internal and external parties simply by sharing a link. So the threat landscape of companies has changed and so it is the way that this data needs to be safeguarded from an availability, integrity, and confidentiality perspective. The security teams of the companies they need to get used not to be responsible for all security tasks anymore. They need to get used to work more with their cloud ERP providers, security organizations, and share the ownership of those security tasks and responsibilities with them. Here is where the concept of trust comes in. Trust means also, For companies getting transparency of all the security measures standards and documentation that those cloud ERP providers shares with them. For example, at SAP we have something called the SAP Trust Center, which is available online, where SAP customers can actually go and find informations on standards, ODES and simply how we run the security processes to secure their data and their business.

Andreas: Yeah, fully agree, but trust might sound a little bit weird in regard to the rising zero trust concept, but indeed, trust is a very important point, and to some extent, we really need to trust the providers that they are doing their job and they are able to do their job. But clients fear to lose the control over their data and they are dependent on the provider. Clients need to stick to some rules of the provider and they need to trust that in case of a service outage, the provider will take care of the issue and is capable to do it. But here we are coming to the next challenge, what clients are facing if a service is not well enough defined there are dozens of ways how our provider can be prosecuted. And, very simple example here is, the availability of a service or the maintenance windows. So if the SLA is on 99.5%, this means that the client accepts an outage of about, let's say 50 minutes or an hour per week. Or, if they have agreed on a maintenance window which falls into the big business time of a specific country, then this can cause issues. And, if you cannot control it or if you cannot move it, you can imagine that this can cause serious issues for the business. Or let me pick up a topic from before. If you're not having a close look at the agreed batching responsibilities, we might not cover all security notes or batches. So there are still some pitfalls which are often overseen, and we need to consider that not all departments, which are dealing with the SLE or agreements, that they are really familiar with security. So it is very likely that security is not covered properly and causes issues if information security teams are not consulted or involved. And, Even if the SAP basis team is not aware enough of security topics, we can also, cause issues or maybe we have some troubles at the end. A further disadvantage can also be the missing comprehensive overview of the cloud entry points in the related assets. So, often they are absolutely underestimated. The hacker needs just one single week entry point to start the attack and compromise the environment. And all considered we need to have a change in a mindset. We need to know our assets. We need to know our environment and duties, and we need to be aware about the changing skillset of our professionals.

Oyku: We have talked about the challenges that companies might face or the concerns they might have. Let's flip the question and talk a little bit about the benefits. So what are the main benefits that companies have moving ERP to cloud from a security perspective?

Gabriele: Yes. And Andres is touching some very interesting points about knowing the assets, understanding the infrastructure, the TET landscape because it is changing in the cloud. And securing business systems and data has always been, complex and very challenging. In the past, even when that was, purely on-premise, it has always required a significant investment in technologies which are expensive, especially to keep up to date. It always required standardized and best practices, processes where you need many

experts from diversified backgrounds to pull it all together. And of course human resources, which are increasingly scars. And here is where I think the cloud brings, opportunities. Starting from the first aspect, which is the people. There is a well known scale shortage in the security industry. And to implement, maintain, and to monitor security, you need to provide 24/7 stuff. And most organizations simply can't afford that. On the other end, cloud ERP providers can attract and retain top talent to support those security operations. If we look at SAP, for example, we have thousands of security professionals and we are keep expanding our teams. We do that by both hiring external people, but we also train our internal teams with security programs and curriculums. And the second aspect is the processes. So companies have managed security for so many years in their own way now with their own internal security teams, which is great because those are the people that know their company best. However, that sometimes impedes security processes to be challenged and innovative. In the cloud, internal security teams are actually supported by external security professionals, which are providing their perspective and industry experience. And in my opinion, this is a very powerful combination because it allows security innovation. And the third and last point is on technology. Again, let's look at SAP for example. We need to manage many cloud ERP environments for our customers, and because of that, we need to comply with all necessary regulations and standards. We are also subject to multiple audits throughout the year. And to achieve all of that, to be successful with all of that, we need to have top notch physical security, but we also need to have the latest technology when it comes to data encryption, controls, automation, threat monitoring, but also disaster recovery and business continuity. For example, in the cloud, we distribute data across multiple data centers and that reduce the risk on-premise systems have of losing their data stored in one data center that could come from natural disasters, fires, explosions, network outages all problems that, on-premise systems of 10 F. And of course, we work together with companies like Accenture who are leaders in the security industry to support our customers best.

Andreas: Yes. We as a service partner and service provider, we can fill gaps of our clients. So, this is really a huge benefit, what we can offer and with a whole bunch of people and several teams which are dedicated to security and the various security areas, which means we can offer the right people and the necessary skills and capacities. But let's go back to some other benefits. When we have a look at the average client, On premise environment, can't hardly compete with the cloud provider. When we are talking about the security of a data center, of course there are a couple of companies out there which have an certified environment. But, I'd like liberty to say the maturity don't have such an environment, so they are not meeting the requirements of, ISO certification or some other standards. And so in general, the cloud providers are usually highly

standardized. And regulated, which provides a good security foundation as Gabs has already mentioned and in consideration of the deployment model and the responsibilities, I would say there is one more huge benefit for the client. Cloud systems might hardly get outdated cause the provider may have some batching responsibilities, which means that this can drive change. We are constantly seeing, many customers, which have issues with a well working patch process. And there are still clients which have unpatched or outdated systems. And, unfortunately this is really allowing me, so this is also a huge threat for the entire environment. With the move to the cloud, I hope this will get much better. You can't escape the user batching cycles in a software as a service or platform as a service scenario. You will be forced to update. And if you are not doing it manually, it'll be done automatically after some period of time.

Richard: Gabs, you mentioned a little earlier that we're seeing a shortage of skill labour. And the demand for data security professionals far exceeds the supply. And if anything, it looks like this gap's growing and that's a scary thought because obviously more and more companies are moving their business systems to the cloud. So what are your thoughts on this? How can we address the skills challenge for security professionals?

Gabriele: Yes, thanks, Richard. And Andreas is, again, touching very interesting points on the tendency on reducing manual operations and replacing those with automation because performing operations manually is no longer an option, like you just said. There is a well known problem in the industry for security, human resources. There's just not enough resources for the demand that companies are having. And it's not just human resources, for me, it's human resources and lack of technologies, investments, which are creating a huge problem when it come to security. And as Andreas was also mentioning in the previous question, The cloud can provide options here. Companies can now take advantage of the people, processes and technologies of cloud ERP providers and their partners like Accenture to reduce this gap and innovate speed.

Richard: Andreas and your thoughts?

Andreas: Yeah, here we have really a serious issue. There are only a few experts and even less SAP security experts, and many of these SAP security experts are focused on SAP authorization. So we have a really huge gap of people with a comprehensive s a security skill and that makes it really challenging for the companies and in our latest Accenture report about global cybersecurity Outlook 2023, which has been presented on the World Economic Forum. At the World Economic Forum reflects the situation pretty well. So

about 60% of the business and cyber leaders are ranking talent, recruitment, and retention as a key challenge for managing cyber resilience. That's a really high number and more than the half of respondents reported that they do not have the necessary skills and the lens to respond to the cyber attacks And I think this really shows clearly that we have an issue and we as a service provider can of course support here because we have many people who can support in these areas and trying to fill the gaps.

Oyku: Mm-hmm. My next question is going to be about, predictions. I haven't seen any application security prediction for 2023. Maybe you can give us your top three predictions for this year.

Gabriele: Alright, go first then. My first one is application security. So application security has been for many years about blocking access to sensitive data. That has been the main focus of security teams, and we will see companies going away from that because application security. Let's be honest, it needs to be better than this. It needs to be less about being a business blocker. It needs to be more as a business enabler. For example, instead of blocking users by default, companies will leverage more continuous monitoring of security configurations, threat detection, as well as automated and dynamic data access blocking, for example, when suspicious user behaviors are identified. All of that will ensure that business can still run a full speed with security running on the site to safeguard it continuously. So that's my first one. The second one, it's cyber risk quantifications. So companies will start to formally quantify the risk of a cyber threat materializing. In their cloud ERP environment, and this is required to provide the board of directors with the info they need to understand all impacts from a cyber risk. And based on that, Estimation, prioritized short-term actions, but also long-term investments to improve the company overall security posture. And my third and last prediction is about managed services. And Andreas mentioned already some of those in the previous questions, especially for application security hardening, continuous monitoring, but also risk quantification. Managed services will be used more and more by companies to enhance their overall security posture. And I think it's about time for companies to start to do that. You know, it's very important to combine the internal security people that they have and the processes and the technologies of course, which they have built in-house with the ones from market leaders organizations who can provide their perspective and their industry experience. This is what companies need now and in the future to manage the cyber risk. And this will be what will give businesses the confidence they need to keep innovating at speed and be resilient on the long run.

Andreas: Yeah, so my top three would be so number one, cyber resilience. Since the awareness of all the cybersecurity risks, which we have around us They're getting more and more aware amongst business leaders and as the overall regulatory security requirements are also increasing such like N two directive GDPR topic or the other act which are published by the European government, for example. It is getting more important, and I think also the audit companies will have a closer look at all these topics in the future.. So, my second one would be zero trust. As mentioned at the beginning with the move to the cloud, the classical bare security is changing. So we are more opening our environment to cloud services, which means we are opening all the firewall ports and, so we have highly interconnected systems with different levels of security, as I've mentioned before. And so we can no longer trust all these environments from an end-to-end architecture perspective. So we really need to be sure that everything is fine. And the last one would be managed service. Customers are missing skills and people, and we as a service provider can fill this gap as mentioned already. So we can enhance customers teams with additional expertise. And of course we can somehow free up their resources so that they can focus on other topics. So yeah, I think this is it.

Richard: So we're coming to the end of the podcast and there's a question that we ask all of our experts, and that is around the future of ERP. So, from a cloud applications and securities perspective, what do you see the future of ERP? Maybe Gabs you could start.

Gabriele: Yes, yes. So I know that question and get ready because I'm gonna be very philosophical on this one. So the way I say it is that the future of ERP resides in being the human best friend. So what I mean by that? The ERP will run besides us. It will learn from us and it will help us doing many tasks of our daily job. Those are all the tasks that we never get to do on schedule simply because we just don't have the time anymore. And this is true of course, in my security area, but it's in pretty much every area of the business because we are just too busy in our lives nowadays. Let's be honest. So the future of ERP is basically making work a happy place to be hardly to save for security professionals. But I think, I hope, and I'm confident that will be the future. And it will enable us to focus on what we really love to do as part of our job. And it will also give us back the time that we deserve to spend in our personal life. You know, that's for sure.

Richard: Andreas, can you beat that one?

Andreas: Oh, no, I don't believe that I can beat this, but I see the future of ERP still be there. So we will not get rid of the ERP environment. When we have a

look at the numbers, about 87% of the global transactional revenue are touching an environment, so it'll be there. I think it just changes. The tasks and activities, what we have. So we are more giving the responsibility to provide us, but we still have tasks to do. And it is of course, still important. And for us, from the security perspective, I think it will be very challenging because we have a lot of tasks to do. We need to do our homework. We are missing experts. We need to clarify responsibilities and so on and so on. So everything is changing and I'm pretty sure we have a long journey to go. But at the end we need to focus on the systems and try to make them secure and, hopefully that we are not getting preached at the end.

Richard: Well, Andreas and Gabs, thanks for a great conversation.

Gabriele: Thank you.

Richard: And I'd like to thank you all for listen. So please mark us as a favorite and you can get regular updates and information about future episodes.

Richard: But until next time from Oyku and I, I'd like to thank you for discussing the future of ERP.