IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

In Conversation with Guido Grillenmeier

Carol Baker

Against a backdrop of surging cyberattacks and governments stepping-up measures to address cybercrime, we talk to Guido Grillenmeier, Chief Technologist, Semperis and Microsoft MVP alumnus for Directory Services about Semperis' latest virtual conference, Hybrid Identity Protection Conference (https://www.hipconf.com) on 1-2 December 2021, and the challenges organizations now face in detecting and remediating security risks in hybrid identity platforms.

Guido Grillenmeier is Chief Technologist with Semperis (https://www.semperis.com).

Based in Germany, Guido was a Microsoft MVP for Directory Services for 12 years. He spent 20+ years at HP/HPE as Chief Engineer.

A frequent presenter at technology conferences and contributor to technical journals, Guido is the co-author of Microsoft Windows Security Fundamentals.

He's helped various customers secure their Active Directory environments, and supported their transition to Windows 10/m365 and Azure cloud services.

Guido blogs at https://www.semperis.com/blog/

Background on Semperis and Guido's role

In Latin, Semperis stands for 'always ready', and it is an ethos we have adopted across the whole of the organization.

As a company we have already had great success in places such as USA and Israel, and as Chief Technologist for Semperis I am helping the company to extend its reach into the EMEA market.

We have invested a lot in our sales and marketing team for the region and it is impressive to see the attention that we're already getting from customers. We have already closed a good number of deals and as a business we are growing at a healthy rate. This expansion is important not only for the business, but also for our customers. We get excellent feedback from our customers about our Customer Support Team. Like our Latin name, 'always ready' we are there for our customers 24/7, 365 days – whether a customer finds themselves in a situation of actually being in a breach, or whether they need help performing compliance testing, or just need help with disaster recovery – we are there 'always ready'.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Companies often find Disaster Recovery challenging – what's your view?

Disaster Recovery planning forms a big part of our service to customers. It's important to remember that disaster recovery should not begin at the time that a disaster strikes. It actually begins far earlier.

When we think about everyone's dependency on technology it is very common to find a range of systems including legacy technology that are all interdependent on each other. When it comes to Active Directory for example, companies have been using this for the past 20 years and it is so ingrained into business processes and applications it is only once a company sits down and does a dry run of a disaster (which we emphasize, everyone should do), that then they realize the humongous dependencies they still have on the so called legacy technology.

At Semperis not only are we helping customers to understand those dependencies, but once they realize the critical impact of being hit by a cyberattack, we help them to get out of such an attack quickly. This is where we help to bring down the recovery time, and help a company get back into business.

Whilst we have all got used to remote and hybrid working during COVID-19, working in this way does come with risks. When accessing business applications you still need to make sure that workers are authenticated to that business application with a proper account. To a large extent that is an Active Directory account – and if that has gone, people will not be able to work, and businesses will stop. In short, protecting identities is the foundation of protecting businesses.

For instance, few businesses would be able to survive a ten-day outage. Whilst businesses will be unable to fulfil customer requests during an outage if we look at sectors such as healthcare it's the minutes and hours that matter.

Whilst there is a 'code of conduct' amongst cybercriminals that they try to prevent attacking healthcare systems, we have seen that pharmaceutical companies remain a prime target for cyberattacks, as recent reports during the development of COVID-19 vaccines have demonstrated.

What about ransomware and the chain of events?

Active Directory is often a target for cybercrime. Once a criminal has access to Active Directory they can move laterally within the networks of the business taking down one system after another reading the data. Companies hold vast amounts of valuable data – critical customer information – and the very secrets of the companies themselves.

During a ransomware attack, data is read from as many machines as possible and instantly encrypted, taking down the operational ability of the business. In this chain of events, if a business is unable to respond quickly by being able to recover a system or detect that such an attack is going on, then then it is in trouble. This is where Semperis comes in. We can help protect the businesses by Advanced Threat analysis of the Active Directory with ongoing checks, and if a company is vulnerable, send out warnings.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

These warnings can be about misconfigurations of the administrations of people that are not Active Directory administrators . Instead, they could be administrators of the application servers which are creating a setting that eventually allows intruders to attack this directory or role. The warning could flag an intruder trying to gain higher elevated privileges by adding a low privileged account to a high privileged group, such as the domain admin for example.

The risk is high that intruders will then be able to take down a complete system and the entire Active Directory. At this point, a business is going to need the fastest possible recovery of that directory. This is where are Active Directory disaster recovery product comes in, and our internal IT promise to our customers is that we will have their Active Directory back within four hours.

Tell me more about your free product 'Purple Knight'

Customers pay us to design, implement and protect in their IT environments. We also have a free tool that allows us to test the vulnerability of their Active Directory without any investment called Purple Knight (https://www.purple-knight.com/). Customers can register to download a very powerful security scanner tool, which they can use to get an insight into the security of their Active Directory.

At Semperis, we always say we scan the directory with the eyes of the intruder – and that basically means the intruder, of course, in the beginning only has very limited permissions. This could have been a secretary account for instance that has been hacked via some malware hidden in an email. These days phishing attacks are getting smarter and whilst we are all aware of this, it is surprising how good the language has become.

In the past, you could spot phishing emails by the use of bad English, but they've become more sophisticated with the cybercriminal using either translators or true native speakers to write the text to lure their victims into clicking that malware. Once the malware is on even a low privileged user, like a secretary, an intruder will be in and will have various permissions to read.

Knowing these vulnerabilities, is of course, the first step in being able to do something about it. That is why we provide Purple Knight for free. It's very valuable to know those vulnerabilities. Whilst it is only a one-time view, with our paid products we are continuously monitoring for new changes that occur, and operational mistakes being made that allow for intrusions to happen. We then warn you directly or remediate those topics right away, but Purple Knight is a great start. And we've been receiving excellent feedback by many companies who hadn't realized just how vulnerable they were.

Your virtual Hybrid Identity Protection Conferences are proving highly successful, tell us more?

Yes, our events are highly successful. At our upcoming virtual Hybrid Identity Protection Conference (https://www.hipconf.com) on 1-2 December 2021 (register at https://www.accelevents.com/e/hipconf2021?aff=ITCIOCEO) attendees can join

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

the well-respected IAM experts and Microsoft MVPs to learn all the latest from the Hybrid Identity world. Engage with your peers to solve complex identity challenges that occur in the ever-evolving business landscapes. The virtual conference will consist of keynote presentations, expert panels, workshops and networking opportunities in an effort to exchange information, share war stories, and ultimately make the identity environments more secure.

I am pleased to say that the Conference has earned its place as the premier education forum for identity-centric cybersecurity leaders tasked with defending hybrid environments. First established in the US, the conference series is designed to advance the skills of IT and cybersecurity professionals through highly technical demonstrations, expert roundtables and networking sessions.

Zero Trust is the name of the game when it comes to preventing malicious actors from stealing the keys to your kingdom – your most privileged accounts – be it on-premises or in the cloud. The Conference will give solid insights into how it is done right. A fully virtual experience, the conference is free to attend, and security professionals can expect to discuss learnings from recent cyber incidents, experiences in recovering from attacks and how to defend modern environments against emerging threats. All sessions will also be available to view for 30 days after the conference has ended.

What is a closing thought you would like to get over to our readers?

I think the key thing is to understand dependencies and perform a dry run. Let's say you have your security teams perform a dry run of an outage. If your complete Identity Management Systems were gone, what does that mean for the business? What does it mean for applications? Whilst there will be some applications that may be safe to use, the majority of the business won't be able to run if people cannot log on to the PCs.

Understanding those dependencies will help companies identify the priorities and know how to protect themselves.. As Active Directory is no longer being serviced by Microsoft in the sense of updates and security improvements (that train has passed and everything Microsoft is doing right now is going into improving cloud services), so the days of seeing improvements in Active Directory security are long gone. This means people need to secure it themselves – and this is where Semperis can help – and we can help anytime.

As I said at the beginning. In Latin Semperis means 'always ready' – and I am very proud to say – we always are!