semperis

iSMG
INFORMATION SECURITY
MEDIA GROUP

# Why Active Directory's 25-Year Legacy Is a Security Issue

**MICHAEL NOVINSON:** Hello, this is Michael Novinson with Information Security Media Group. We're going to be discussing Active Directory in '25 with Mickey Bresman. He is the CEO of Semperis.
Good morning, Mickey. How are you?

**MICKEY BRESMAN:** Great. Hey, Michael. Good to see you.

**MICHAEL NOVINSON:** Really nice to see you again as well. I wanted to start you off by getting a sense of this milestone for Active Directory. I know it just turned 25-years-old. I wanted to start by getting a sense of what is the significance of that anniversary for identity security?

**MICKEY BRESMAN:** I think, if you think about even in more general terms, there are not that many technologies that at least I'm aware of that have lasted for 25 years or more. This, by itself, is a very amazing achievement. I think it speaks volumes to how great the product actually was. Because if you think about how many technologies do you know that have been around for 25 years or more, I bet you that you can count those on one hand.

Active Directory is one of those that have been around now for 25 years. I think when it came out, it created this new motion of being able to manage and secure all of your identities in a single location, which I think is what made it so unique. That's also why it is still up and running. I think also, some of the things that were built in into the Active Directory, if you think about 25 years ago, build a solution that have some resiliency already built into it for the replication mechanism, as an example, was groundbreaking. I think we still benefit from that even today.

**MICHAEL NOVINSON:** On the flip side, as you said, it is a quarter of a century old. What are some of the inherent vulnerabilities in a 25-year-old identity management solution?

**MICKEY BRESMAN:** For sure. If you think about the fact that it's been around for 25 years, that means that the world in which it was created was very, very different from what we're living in today. What I mean by that is that individualization was not really a thing yet. Definitely remote work, cloud applications, none of that existed. A lot of the new technologies and the way that the architecture of the modern enterprise looks like is very, very different.

More than that, 25 years ago, some of our assumptions were how do you actually use Active Directory. What I'm referring to is potentially we used to think that domain is one of the functions inside of the Active Directory. We used to think that that is a security boundary, which over the years was proven to be obviously not the fact.

**"Most AD environments have been managed by different people over the last 25 years."**

Another thing is I think that also have changed over the years, and that should happen with any technology that's been around for 25 years, is that multiple different people, administrators, have been configuring the Active Directory for different purposes. One might have some thoughts on what he or she would find to achieve with the Active Directory that potentially have been changed by somebody that inherited. Then fast-forward to where we are now, most AD environments have been managed by different people over the last 25 years. You'll have at least five or six different administrators that were managing the environment.

In many cases, it means that people are not really sure why this thing is there, why we have this type of a configuration. In many cases, they have a lot of concerns of potentially changing something because they're afraid of, "Well, I don't know what's actually going to break because these things have been this way for the last 20 years or so." That's a very distinct scenario that we see with many companies.

**MICHAEL NOVINSON:** How are adversaries increasingly targeting vulnerabilities in Active Directory?

**MICKEY BRESMAN:** Yeah. If you think about it, Active Directory is still the core of identity storage for 90% of the companies out there. What it means now is that from the adversary perspective, if I want to breach your Salesforce as an example, I'm actually more likely to go after your Active Directory. The reason being is because of the things that we just mentioned. I know that your AD have been around for more than 25 years. I know that it has been managed by multiple different people in the organization, the administrator function. And I know that potentially you have vulnerabilities that were created over the years and that you were afraid to touch upon.

One interesting example can be service accounts. Service accounts in most companies today, they have I believe more service accounts, or something referred to as the machine identities or the non-human identities, than they have actual humans in the organization and it's a significant difference. In many cases, those service accounts were created years ago. In some of the companies that we work with, we see that because of that, they had exemption on what the possible policy should be. Data companies have a more complex policy of 10, 12 characters or more, because typically today you would use an expression, you will still see service accounts that were created 10, 15 years ago, before we had any policies. Those have six characters only. Because of this inherent concern that people have of, "Well, I don't know where this service account is being used, I don't want to touch anything because it might break something in the organization." It obviously creates this situation where those become relatively weaker accounts in the environment.

Now service accounts and other parts of the Active Directory tend to be privileged accounts. If I get a hold of those, I can do a lot of different things inside of your environment all of a sudden. Active Directory have been many times described as, and rightfully so, as the keys to the kingdom. Which basically means that once I get a hold of your AD environment, I can do whatever I want in the organization.

Going back to the Salesforce example, it's actually easier for me to go after your Active Directory, get a hold of your AD environment and then through the different synchronization processes, simply to log in into your Salesforce environment. This is something that we see, and not just us, you will probably hear from multiple different analysts and different security firms out there that in eight out of nine, or nine out of 10

attacks out there, Active Directory is going to be right in the middle of it because again, it's been around for a long period of time. If you're not properly maintaining it, then it's going to have security issues in it. The most interesting part is that once I really get a hold of your AD, then I can do a lot of different things in the environment.

**MICHAEL NOVINSON:** I wanted to get a sense from you as well, in terms of where do you feel that enterprises are consistently falling short when it comes to securing Active Directory?

**MICKEY BRESMAN:** Yeah, that's a great question. I think one of the things that we're seeing is a lot of built in concern. The concern that I'm referring to is not just the concern about AD security. I think today … Maybe I'll just step back.

I feel that the industry today got to a point where there's a very good understanding of the criticality of AD. There is a very good understanding of the security and the need to make sure that our AD is as protected and as secured as possible. From that perspective, I feel especially over the last three years, there's been a huge jump in the industry.

I think there is still a lot of concerns, and in some cases those concerns lead to not necessarily the best behavior, as the example that I used before with service accounts. But we actually see those with other configuration issues in Active Directory as well, where some organizations don't fully understand what potential exposures exist in AD environments. In some cases, they might understand the exposures, but they're not really sure what to do about it. They have a lot of concerns of, "Well, this thing, again, has been around for more than 20 years. I make a change and then something breaks."

In some cases, I think some organizations also don't fully understand the impact of the AD environment on their cloud infrastructure, as an example. How things actually are working, and how is it tied? What will happen if a breach in AD, what implicate it will have on their cloud infrastructure or SaaS applications? I think in some cases, we still see organization that trying to better understand if my AD becomes unavailable as an example, it goes away in a ransomware attack. What happens to my cloud infrastructure?

We see a lot of those things that people are trying to understand. But to your question, I feel that there is still a ways to go until we'll get to a point where people fully understand and know what to do about it.

**MICHAEL NOVINSON:** Let's talk a little bit about Semperis. Specifically, I'd love to get a sense of your rise, the success, as well as your ties to securing Active Directory.

**MICKEY BRESMAN:** For sure. Semperis, as you probably are aware, has been on a very successful trajectory path and we're super excited about it. We've been on the Deloitte 500 Fastest Growing Companies I think for the last four or five years in a row now. We've also announced last year that, at the beginning of this year I'm sorry, that last year, we have crossed the 100 million ARR mark, which is a very significant milestone in every company's journey obviously. I think it makes us probably the biggest in independent identify detection and response company out there.

**"Some organizations don't fully understand what potential exposures exist in AD environments. In some cases, they might understand the exposures, but they're not really sure what to do about it."**

One of the terms that we're actually now using as well to help people better understand what is that we can actually provide is identity forensics and incident response. On the same token of data forensics. Well, DFIR, the data forensic incident response, is a more common practice. I think IFIR, the identity forensic and incident response is a newer one. But if you think about it, the dependency on identity and how things have changed, especially with cloud adoption and remote work, we'll see more and more focus on the identity as the perimeter. We hear about it all the time now.

I think that also, to your question, in some cases when people think about incident response, in the case of the Active Directory, they sometimes might not fully understand the scope of what an incident response for Active Directory actually means. What I'm referring to is that if you simply recover an Active Directory following a ransomware situation as an example, you are actually leaving a lot of back doors that can be used by the bad actors to take your environment down again. Because in order for me to take down, to encrypt your Active Directory in the first place, I need to have a privileged account in your environment, that's a given requirement. Otherwise, I will not have the permissions in AD.

I think one of the things that we're now trying to, I don't know if educate the market is the right term here, but trying to bring attention to is that IFIR, identity forensics and incident response, is a very significant practice that organizations needs to pay attention to.

**MICHAEL NOVINSON:** How are you best helping your customers ensure a secure future?

**MICKEY BRESMAN:** Semperis is uniquely positioned in the fact that we are actually covering the entire attack cycle. We're doing the pre-attack, the during the attack and the post-attack. We're doing it across both the on-prem and the cloud environments. Meaning that we have offerings that start in AD, but then expand into Entra ID. We also have coverage for Okta.

Where we help customers is with the pre-attack stage, helping them to find as many of the vulnerabilities possible before the bad actors takes advantage of those. We are also, to the question and to the point of Active Directory being around for so many years, many of the organization have a technical debt when it comes to the Active Directory, especially if they've been acquiring other companies. They find themselves in those scenarios where they're all of a sudden managing 20 different AD forest environments. All of those connected with trust between them where, as you can probably imagine, the weakest of those security AD-wise can be used in order to compromise the entire organization. I need to basically bridge one of those and use it as a bridgehead. We're also helping companies to consolidate those environments and to move those to a more modern type of an architecture that is a bit easier to defend.

**“Many of the organizations have a technical debt when it comes to Active Directory, especially if they’ve been acquiring other companies.”**

Then we’re also helping companies the during the attack stage. Identifying when they’re being attacked, how to see what the adversary is doing and how to detect and basically contain it as fast as possible.

Obviously, what we are most known for is what happens in the worst case scenario. If you’ve been encrypted end-to-end, or the more likely scenario, the bad actor got a hold of your AD environment and you can’t seem to get rid of the adversary, that’s where our incident response team comes in. Or I should probably start saying IFIR team comes in, because we can help find what the bad actor has actually been doing. We can help isolate them and then basically make several steps that will eventually help the organization to get rid of those adversaries in the environment.

**MICHAEL NOVINSON:** Finally, here I wanted to get a sense of where do you see the putt going? Both for Active Directory, as well as identity security.

**MICKEY BRESMAN:** That’s a great question. I think it would be interesting to see if we were having a call in 25 years from now, my bet that Active Directory is still going to be around, as interesting as it sounds. I think we definitely could see an expansion of organizations into the cloud identity providers as well. We see in most cases that being in addition to Active Directory and not instead. Some companies have requirements that actually forces them to have an on-prem IDP, identity provider, which AD is the most common one for those.

But we also see a big push from organizations to try and modernize the identity stack, and in many cases the move to the modern authentication protocol, some of that type of protocols, which requires you to rewrite many of your lines of these applications. But I suspect that that’s what we will see more of. We will see more and more organizations being able to rewrite those applications and get to a point of working with the cloud IDPs.

**MICHAEL NOVINSON:** Absolutely. It definitely will be fascinating to watch in the years to come. Mickey, thanks so much here for the time.

**MICKEY BRESMAN:** Thank you, Michael. Good seeing you.

**MICHAEL NOVINSON:** Same here. We’ve been speaking with Mickey Bresman. He is the CEO of Semperis. For Information Security Media Group, t his is Michael Novinson.

## About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 36 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · CU INFO SECURITY® (Just for Credit Unions) · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk TODAY · CAREERS INFO SECURITY® · Data Breach TODAY (Prevention. Response. Notification.) · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io