AN INTERVIEW WITH WITH MICKEY BRESMAN, CEO, SEMPERIS

CYBER RESILIENT IDENTITY ENVIRONMENTS FOR ENTERPRISE

The importance of Microsoft Active Directory (AD) in enterprise IT infrastructure is clearly understood by practitioners—and this has extended more recently to security teams. Much of this new security emphasis around identity and directory services has been on the potential for attackers to use infrastructure to accelerate enterprise breach campaigns. This usually involves increasing privileges through poorly configured AD deployments.

An often-overlooked threat, however, involves catastrophic breaks in directory services. These can originate from malicious attacks, and also more unintentional administrative mistakes. In either case, the consequences can be severe, often requiring lengthy periods of recovery and restoration. Any enterprise practitioner will immediately understand the implications of directory service outages. In most cases, the entire business will operate in a severely degraded mode.

The TAG Cyber team recently sat down with an expert in this area. Mickey Bresman, CEO of New York-based Semperis, explained to us how his team offers Active Directory recovery services, along with protective capabilities that help customers avoid the identity and challenges referenced above. As should be evidence in the interview below, Mickey emphasized how automation plays a critical role in the resilience process.

TAG Cyber: What are the primary threats to Active Directory that your team addresses?

SEMPERIS: In my conversations with security executives and practitioners alike, AD is frequently referred to as the "Achilles' heel" of enterprise security. Not only does it hold the keys to the kingdom—it's a treasure map for attackers. And being fundamental to the IT infrastructure, if AD is encrypted or wiped out, business comes to a screeching halt. Unfortunately, AD is very difficult to secure, given its constant flux, the sheer number of settings, and the attackers' easy access to powerful hacking and discovery tools. Further, ransomware attacks have quickly evolved into highly targeted and extremely damaging network-wide infections that can proliferate through AD. To put it plainly, AD was built 20 years ago, and although it stood the test of time, it can't stand up against today's threats on its own.

In our mobile-first, cloud-first world, any connected device can expose the heart of your IT infrastructure. In fact, you should assume that attackers are already lurking inside of your AD and just waiting for the opportune moment to strike. With this in mind, defenders must anticipate their adversaries' advances and thwart off AD attacks at every stage of the cyber kill chain. Semperis delivers comprehensive threat mitigation and cyber resilience for AD. Our patented technology for AD protects over 40 million identities from cyber attacks, data breaches, and operational errors. We deliver defense in depth across the full attack continuum—before, during, and after an attack.

TAG Cyber: Tell us about the algorithms you use to accomplish this recovery and protection. How do they work?

SEMPERIS: A typical Active Directory is in a constant state of flux, with hundreds or even thousands of changes made each day, which makes securing AD a proverbial "moving target." To maintain control of AD, monitoring must occur on two fronts: (1) security posture of AD (how objects are configured in AD to protect against attacks) must be monitored, and (2) changes to AD must be monitored with the ability to auto-remediate sensitive changes for round-the-clock protection.

Semperis continuously monitors for indicators of exposure and also consumes the AD replication stream and native Windows security event logs to capture changes to AD that could result in security compromises. Semperis monitors all aspects of AD, including integrated DNS, Group Policy, sites, and subnets, etc. The unique part of our approach is in the completeness of the solution. In the pre-attack stage, we provide our customers with new templates of indicators on a continues basis. Semperis offers customers built-in threat intelligence from a community of security researchers—our own and from the general community. If a new type of an attack vector is discovered, we will provide customers with a new template to simply import via PowerShell and from that moment on, the system will monitor for the new threat.

On the disaster recovery side, Semperis introduced the first backup and recovery solution purpose-built to recover AD from cyber disasters like ransomware and wiper attacks. When your business is down, every second counts and complexity is your enemy. Semperis fully automates the AD forest recovery process to avoid human errors and reduce downtime to minutes instead of days or even weeks. Our patented technology separates AD from the underlying Windows OS and only restores what's needed for the server's role as a DC, DNS server, DHCP server, etc. —virtually eliminating the risk of malware re-infection during restore.

TAG Cyber: Do you see much difference between malicious attacks on Active Directory and inadvertent administrative errors? Do they have the same potential impact?

SEMPERIS: Yes, there is a big difference between the two. From my perspective it comes down to trust. Do you know what hit you? Do you trust your backup? How about the Windows that your AD is running on?

In the administrator error scenario, you know (hopefully) what happened and can reuse parts of your infrastructure. In the malicious attack scenario, you can't trust Windows, and if your backup includes big parts of Windows (like in the case of system state and bare metal), you can't trust your backup either. We

And being fundamental to the IT infrastructure, if AD is encrypted or wiped out, business comes to a screeching halt.

have witnessed scenarios where the organization will spend days to restore AD, just for it to go down again soon after the recovery. So, although the damage of downtime is as painful in both scenarios, recovering from a malicious attack requires a different approach. Also, keeping in mind that a malicious attack might mean that the attacker has hold in your AD (privileged accounts) and not just the Windows (malware).

As the cyber threat became the much more common scenario, by default we assume the worst in our approach to recovery, with a share nothing, trust nothing state of mind.

TAG Cyber: What are some of the restoration improvements you see for enterprise customers? How much more quickly can they recover after a problem?

SEMPERIS: Semperis puts AD recovery on autopilot, empowering customers to respond more effectively to security incidents and everyday operational mistakes. With Semperis, customers shorten the recovery time of their entire AD forest by up to 90%. Being a fully automated solution, Semperis removes the dependence on resource-intensive and error-prone operations. We pride ourselves on delivering the fastest, safest, and easiest AD recovery solution on the market. The solution's end-to-end automation orchestration process frees up teams to allocate more focus on other aspects of the business. Here's one of our favorite customer quotes from the InfoSec Identity and Directory Lead at a F100 Global Retailer: "When I saw the Semperis solution for the first time, it nearly brought tears of joy to my eyes. It is exactly what I hoped for in an AD recovery tool. Over the years, I've had numerous concerns about forest recovery, and Semperis addresses them all."

TAG Cyber: Is real-time visibility into directory service infrastructure one of the benefits of your solution?

SEMPERIS: An attacker seeking persistent privileged access in Active Directory will typically attempt to bypass security auditing in some way. Security and auditing solutions like SIEM rely on either a native auditing agent on every domain controller (DC) or on security event logs (or both). But an attacker can circumvent auditing in any number of ways, including deleting the event log, stopping the collection agent, and turning off auditing. Sophisticated attacks can also bypass security auditing altogether. For example, the DCShadow attack technique injects changes directly into the AD replication stream.

Semperis leverages multiple data sources, including the AD replication stream, to provide uninterrupted visibility and capture changes that otherwise will go unnoticed. So even if the change was made while the auditing agent on the DC was down, and even if the security event logs were destroyed, our customers will still have the visibility into the modifications made in the environment. On top of that, we provide the auto remediation capability, where the system can take the decisions to undo a change or take an action like disable an account and have the security analyst investigate.

TAG Cyber: Any final thoughts on the future of identity and directory service integrity and resilience for enterprise?

SEMPERIS: Organizations are going through a massive digitalization change. Software as a service adoption, WFH, BYOD, and other business trends changed the IT security concept of being in the same perimeter, behind a firewall, with organizational policy on the organizational devices. Many have said that identity is the new perimeter in this new world and I couldn't agree more. In Semperis we believe that world is going to be hybrid for a very long time, with line-of-business applications running both in the data center and being adopted as a service. Hybrid scenarios and cross cloud scenarios (using Box with O365, for example), will be dominant in the future. In this new world, protecting identity across multiple providers will be crucial to the organization's security, compliance, and operation. Identity is already a command and control in many aspects, but also a lucrative target for an adversary ("keys to the kingdom"). We want to make sure it's secured, protected, and can be easily recovered in the worst-case scenario, no matter where the attack came from or how severe was the damage.