How Windows Active Directory is the root cause of many logon security headaches

By François Amigorena, CEO, IS Decisions

Managing access to corporate networks is one of the most important parts of an IT professional's job. The reason why is simple. Poor access security can lead to devastating data breaches, like that of Dropbox, eBay, Sony, Anthem, Sage, Three and many others. These attacks occurred as a direct result of an employee's login details falling into an attacker's hands.

And yet, despite these attacks, many organisations are doing very little to shore up their user access security, with many still relying on standalone native Windows Active Directory (AD) to do the job. A great many experts agree that using AD on its own is incredibly risky. Analyst and director Bob Tarzey at Quocirca argues*:* "Active Directory provides basic user security, checking that credentials supplied match stored user profiles and then opening up access to resources. Stronger techniques are needed to ensure a user really is who they say they are."

Those companies that use AD on its own are now facing huge challenges, as IS Decisions has found when delving into online community forums like Peerlyst, Spiceworks, Reddit and DaniWeb.

Many community members have been quick to point out AD's limitations. A man who calls himself "Guurhart", for example, believes "the biggest challenge is Kerberos and the weaknesses inherent in AD. Only the latest versions of windows give you any real chance at beating attackers who're trying to move laterally."

Scott Miller from Niagara Technology Group adds to this saying: "A major limitation of AD is the assumption that you will have a LAN. Azure AD (which is not AD) breaks this barrier and is worlds better as a concept. Unless you are totally LAN centric, AD adds so much complication."

Brad Voris also comments on the inflexibility of group logs, saying: "Audit logs are in the form of event logs with specific error messages, some of which require Group Policy configuration changes on the Domain Controller Default Policy. Initially there is VERY limited logs and in order to get more data you have to make a fair amount of changes to Group Policy. Very important."

Indeed, a previous piece of IS Decisions research in The Insider Threat Manifesto found that nearly half (49%) of IT security professionals believe there to be security holes in AD.

And on the community groups, when asked what's the worst that could happen as a result of poor user security, another member said: "Social engineering, gathering data, installing software, running ransomware on shared resources" — no doubt a terrifying prospect for any IT administrator.

Most of these scenarios stem from the fact that AD can't defend against the use of stolen logon credentials. It can't stop careless user behaviour such as password sharing or concurrent logins. It doesn't let you apply temporary logon controls. It doesn't ensure access is identifiable and attributable to an individual user. It can't monitor systems in real time to get a clear picture of who, when and where is on the network at any one time. And there's no auditing with centralised, network-wide reporting, which means it can't detect possible or suspicious access events.

The restrictions of AD are leaving organisations at a loss at what to do, and many organisations are not going about fixing the issue of AD in a logical way. Some are completely overhauling their security systems. Brad Voris says: "My organization is implementing a massive new security program and overhaul to change not just the physical/logical aspects of security but also the culture."

Some companies have ruled out real-time monitoring on the mistaken assumption that it is too time consuming and difficult. Guurhart says: "Keeping up with who's doing what in real time seems like a pointless exercise that will drain your IT and infosec staff rapidly."

Most shockingly, many are sticking their head in the sand and doing nothing due to a lack of budget to fund access security. Roguetroll says on Reddit: "We use Windows Active Directory. But since there's no budget for security (I don't even know if we're running AV on all machines right now) let's just say we're deploying the "told you so" method when shit hits the fan."

So, what can organisations do to improve the user access security beyond using AD? Brad Voris argues that because "there's no real native support for MFA/2FA, third-party tools should be used" and Guurhart argues that it's "very important to get an alert when certain access events occur. When detected or alerted, you need playbooks for handling these situations. If you don't have playbooks and someone trained in using those, you will respond inconsistently and randomly."

Technology like UserLock exists now that can run alongside Windows AD to plug the growing number of security holes with regards to user access. These tools can restrict logons to a combination of particular workstations, geographies, mobile devices, times of day and more — whatever the IT department deems fit — to close the window of opportunity for would-be attackers. Should an employee's login credentials fall into the hands of an attacker, that attacker would likely attempt to log in outside of the restrictions set up by the IT department. This kind of security minimises the damage of a number of attack vectors like phishing and ransomware. But not only does it halt outside attackers, it can monitor and audit everyone on the network and attribute network activity back to each user, which many regulations like SOX, PCI DSS and more are beginning to get hot on.

The one thing to take away from this article is that Windows Active Directory on its own is not an effective way to manage users on your corporate network. Your data and networks are far too valuable to be put at risk by systems that weren't designed with access security in mind. Third-party tools are the key.

About The Author

François Amigorena is the founder and CEO of IS Decisions, a provider of infrastructure and security management software solutions for Microsoft Windows and Active Directory.

IS Decisions offers solutions for user-access control, file auditing, server and desktop reporting, and remote installations.

Its customers include the FBI, the United Nations and Barclays who rely on IS Decisions to prevent security breaches; ensure compliance with major regulations; such as SOX, FISMA and HIPAA; quickly respond to IT emergencies; and save time and money for the IT department.