Highlights from a recent webcast on security for AD Groups

HOW POOR (OR LAX) AD GROUP MANAGEMENT BECOMES A TARGET FOR HACKERS

Security breach numbers keep going up: More than 5,200 were recorded last year, according to the 2017 Data Breach QuickView Report, up from 4,149 in 2016. Hacking continued to reign as the leading breach type, too. Understandably, the risk of breaches highly influences security spending. As organizations react to high-profile cyberattacks and data breaches, Gartner Inc. forecasts that enterprises will increase their expenditures on IT security technology and services to total $96.3 billion in 2018.

Yet companies may not be covering all the bases when it comes to thwarting malicious activities. Often, they underestimate hackers' attraction to Microsoft Active Directory security and distribution groups as both targets and lures, and thus fail to vigorously manage all of them – such as those groups composed primarily of average user accounts that are not highly privileged.

In an AD security group, it isn't difficult for attackers to obtain a security identifier (SID). With a security principle they control present in a permissions group, would-be hackers can gain access to user rights and shared resources, putting the enterprise world at their disposal. Or, they can infiltrate mailing list groups to gather intelligence about the corporate environment that can bring an air of legitimacy to the social engineering attacks they plan to launch. They may learn, for example, how to make a credible request to the help desk to place an account they're plugged into in a certain security group.

Perils of Skimping on AD Group Management

It's fair to state that IT does a good job locking down domain and enterprise admin AD groups, as well as some security groups. But it's equally true that very few of the hundreds or thousands of other AD security and distribution groups that exist in a typical business are considered high-risk enough for IT to dedicate expert staff time to accurately maintaining and stringently auditing them. Hackers count on that, and the modifications they effect upon these groups tend to be a result of their social engineering successes and businesses' human management failures – not malware.

That said, AD group hackers can set loose malware with far-reaching consequences. Not long ago, for example, an employee at a $2.5 billion company was using a computer that – unbeknownst to all – had been infected by malware targeting Outlook thanks to an AD distribution list group hack. Each piece of email the employee received was copied off the network to another point. That included diagrams depicting the business' newly rearchitected network, which provided the hacker with all the IT infrastructure and security information needed to deploy other malware into the environment to breach the enterprise's customer database.

Not only was the attacker able to pull down tons of customers' information, including their payment details, from that system, but it also used the data to launch social attacks on those clients directly, compounding the already significant damage. The event ultimately cost the business about $220 million.

Improving the Management Situation

Fortunately, there are procedures that enterprises can leverage to lessen the risk of hackers successfully exploiting AD permission and distribution groups as attack points, as well as tools they can use to more efficiently address those process changes.

■ As a first step, businesses need to address the problem of old security principals lingering on as accounts in security groups where they no longer should exist. The more SIDs in a group, the broader the attack surface and the easier it is for a hacker to find the weak point – say, the SID with the terrible password that's as easy to crack as an egg.

Regular audits, preferably handled by the AD group's data owner, can ensure that users whose roles have changed no longer live on as SIDs in their groups. Admittedly, it may be necessary for IT to deploy an interface that forces data owners who aren't eager to do the job to follow through on audit actions. The need for such a custom self-service UI almost always requires the use of third-party tools, such as Imanami's GroupID Self Service module for delegating AD

administration to end users.

Education also must take place to ensure that auditors realize that the process being put in place creates a point of accountability, should careless enforcement on their part lead to corporate data loss or other damages from a hack that successfully compromises an old account.

> It's advisable to conduct AD security group audits daily—maybe even twice a day—so that your business stays ahead of the hackers.

■ Alternately, it may be possible to deal with old SIDs via the option of applying automated membership, populating AD with canonical personnel information —such as data relating to a user's job title, department, supervisor and so on—from an HR system. Corresponding AD groups then can use these AD attributes for their own auto-population purposes. So, when personnel data changes are applied to the HR system they also will propagate down to AD, and from that point group memberships automatically can be shifted, too.

This population of AD attributes with canonical personnel data to automate group maintenance can happen in various ways:

• Creating PowerShell scripts, though that can be clunky depending on staff expertise with the systems with which AD must synch. Additionally, since PowerShell scripts run on a schedule, there will be a delay in populating and depopulating AD groups.

• Custom-coding in a lower-level language such as C#, though this will require maintenance over time and therefore continued commitment.

• Using a third-party tool that requires only a single installation and one set-up process for synchronization. Among such solutions, Imanami's Active Directory Group Management suite includes synchronizing of data sources with AD. Third-party tools like this one that are subscribed to an AD Event Queue also can dynamically and more immediately populate AD groups than PowerShell scripts.

■ Next, most distribution groups should be subject to the same above treatment as security groups. A tremendous amount of IP and other sensitive and high-risk data still travels across the company by email, so IT must ensure that data owners conduct regular group audits or automate memberships, if possible, in mailing list groups, as well.

■ Of course, true low-risk distribution groups do exist, whether for the company holiday party or its annual charity fundraiser. These don't warrant a similar degree of valuable human time and attention. In these cases, it's better to deploy self-service portals to allow users to self-manage their membership. Importantly, users in charge of these lists should also modify these group names to make it clear that they are unmanaged, low-risk distribution groups – just to ensure that no one accidentally uses them to pass around the payroll spreadsheet, for example. Third-party solutions like Imanami's GroupID support features such as enforceable naming conventions for such scenarios.

■ It's wise to take advantage of group health monitoring for all your AD groups to discover problems such as groups with many disabled user accounts, poor descriptions or no points of contact. Such issues suggest an ad hoc rather than formalized approach to management and likely mean that more security problems are lurking due to lack of process and visibility. Tools, like Imanami's free measurement and reporting tool GroupID Health Meter, can scan through groups to uncover actionable points to address.

■ Let IT manage the groups – likely the most important in the organization – that truly require the highest degree of human expert attention, leaving the others to data owner administration and automated and self-service membership where possible with the help of third-party custom self-service UI tools. That way, finite IT resources can focus their attention where it needs to be.

It's critical for companies of every size to realize the importance of taking steps to ensure that their AD groups are not neglected when it comes to securing the organization against potential breaches. It's time to acknowledge that AD groups are a true point of vulnerability – even if just by providing a stepping stone for hackers to get at other assets.

Remember: Every organization is a target for attack in almost every manner imaginable. Whether that hack will result in a successful security breach is in each business' own hands.