Don't Neglect the Role of Active Directory in Cyber Defense

Why an Active Directory disaster recovery plan is crucial for cyber resilience and security in state and local governments

Microsoft networks use Active Directory to authenticate users and grant access to business resources like applications, databases and files. Neglecting the proper backup and recovery of an Active Directory dramatically increases the cyber risk level for government agencies.

*How so? We put this question to **Brian Hymer** (above left) and **Bryan Patton** of Quest Software, which specializes in managing, modernizing and securing enterprises and government agencies. Hymer is a solutions architect and Patton is a principal solutions consultant.*

Why is Active Directory such an important part of disaster recovery, and why do state and local leaders tend to overlook it?

Hymer: Active Directory is the primary way users in most organizations authenticate and authorize access to all the business resources their people need. Without Active Directory, it doesn't matter if you restore the other pieces because nobody has the authorization to reach them.

Patton: Many people think they are already covered because their disaster recovery solution has a checkbox for Active Directory. What they fail to realize is some of those solutions only restore data (objects) in the directory — but cannot restore the directory.

Hymer: If they fail to back up and recover Active Directory properly, then they will probably fail to recover the rest of their environment.

How does the current threat environment make it more imperative to recover Active Directory effectively?

Patton: Ransomware gangs are on the rise — searching for affiliates to infect networks. It's not just external people to worry about. It may be somebody internal who's not getting paid very well who wants to deploy a malware payload.

Why do traditional backup solutions fall short for recovering Active Directory during a cyber event?

Hymer: With Active Directory, it's not enough to restore a domain controller to a healthy state. Traditional backup solutions don't understand how to re-sync Active Directory domain controllers. It's not an easy task. Microsoft outlines some 40-plus steps which must be carried out on each domain controller — and coordinated across all domain controllers.

Patton: And it's not just restoring the directory: It's kicking the attackers off the directory. If a Zero-Day exploit was used, then it's likely that malware is sitting in your backup. That has to be part of your plan.

What else should government IT leaders be thinking about for Active Directory restoration?

Patton: Practice your recovery. Practice every single domain controller going down, then restore them. Active Directory is designed to be highly available. If one domain controller goes down, another one picks up the load. Most organizations across the world have not tested all their domain controllers going down at the same time. Practice that scenario so you have a chance of restoration.

Hymer: Make sure you regularly back up your Active Directory offline — airgap it. Because if it's still on the network when ransomware hits, then it'll get encrypted with everything else. It could be as simple as backing up to a USB drive you keep in your desk drawer. If you back up your Active Directory there once a week, you are in far better shape than if you have no backups at all.