

Active Directory Health Check

Active Directory Domain Services (AD DS) is the core identity platform in many organizations which provides central authentication for users and devices. **Therefore, it is no surprise that an attack on Active Directory is one of the main targets in cyberattacks**, where hackers can gain complete control over your system, which can have a tremendous impact on your business.

Many current AD setups were designed ten or more years ago and IT often forget and ignore on the entire AD Design also during migration of operating system.

Advanced security solutions are normally coming with the high price but there is room for the improvement within organizational environment itself. **Why not fully utilize tools that are already available within your organization to reduce and limit potential attacks significantly?**



How to protect your organization?

- Reduce the possibility of credential theft.
- Removing vulnerable protocols and security holes.
- Protection of employees' devices.
- Active Directory Optimization.
- Delegation of custody rights.
- Inspections done on the regular basis.
- Use of existing tools.

ADD Active Directory DS Health Check Includes:



Identification of the anomalies and safety gaps



Check & Findings report



Guidelines and assistance for anomalies and gaps eliminations

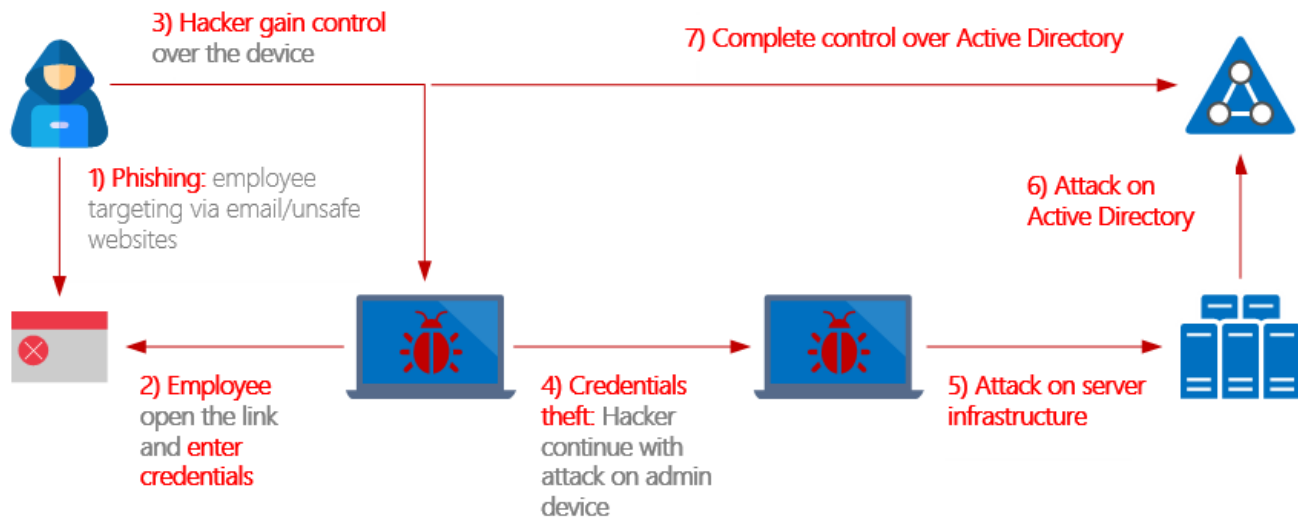
Use your existing tools and capacity for threats eliminations.

How it works?

During the investigation process, we position ourselves into the attacker's skin. We are checking possible ways to obtain essential credentials to gain access to important data and information. We identify security gaps that are relatively easy to fix with existing tools and processes within the active directory during this process. After investigation, we prepare and present a final check & findings report, including guidelines for increase the protection of your information system.

We built the AD Health Check framework with pre-defined steps & activities based on many use cases from the real-live when we helped recover different organizations after AD attacks.

Example of an attack on Active Directory



Why ADD?

In ADD d.o.o. we have extensive experience in troubleshooting and resolving minor to significant hacker attacks through the theft of credentials in Active Directory/Azure Active Directory. With our expertise, we protect IT environments of various sizes and reduce the possibility of cyberattacks. Security checks are performed by a team of experts with certifications from the protection field in Microsoft environments.

