Success Story

TLC for a Long-Neglected Active Directory

Midwest Healthcare Network

"We know we're a mess, but we don't know where to start."

That was how the security team of a Midwest hospital network started its conversation with STEALTHbits' Professional Services team. And they weren't kidding.

Explained STEALTHbits' Senior System Architect, and a Professional Services Team member, Ian Anderson, "Over the years, we've seen a number of Active Directory and File Share environments in disarray, but this one was in really bad shape. But, at least they were aware of it, and knew where to turn."

Their healthcare network included 6 hospitals and 40 total locations, and is subject to HIPAA regulations. They asked STEALTHbits Professional Services team to evaluate their current environment, report on security issues, assemble a list of the highest priority items, and make remediation recommendations. The two-month project was an eye-opener for both the hospital's security people as well as STEALTHbits' Team.

Among the Active Directory issues the Professional Service team discovered, no password polices were being enforced. Anonymous users were allowed to authenticate to the root of their domain, and a number of servers had no group policies applied, so no security policies were being pushed to several servers.

"Maybe the most dangerous issue we found, however, was the membership in groups with elevated privileges," added Ian. "There were more than 35 permanent members of the Domain Admin group, 20 in the Enterprise Admin group, and 5 in the Schema group. Those Groups should be empty, or have one or two members, worst case."

In addition, nearly 900 AD accounts had no password requirements, so the passwords could be blank. Moreover, over 1,500 accounts had no password expiration policy. "We found one password that was 17 years old," revealed Ian.

In Brief:

- Midwest Healthcare Network
- 40 Locations
- 6 Hospitals
- Active Directory was completely neglected

Quotes:

- "We know we're a mess, but we don't know where to start."
- "There were more than 35 permanent members of the Domain Admin group, 20 in the Enterprise Admin group, and 5 in the Schema group. Those Groups should be empty, or have one or two members, worst case."
- "We found one password that was 17 years old."

The STEALTHbits Professional Services effort extended beyond Active Directory into an analysis of the Hospital Network's File shares as well, and the results were no less astounding. First, STEALTHbits discovered 45 servers completely ungoverned by security policies, 30% of all file shares were open, and 98 open file shares granted full permission to all data, read/write/delete. Added Ian, "They also had a number of local user accounts in the Local Admin group, so that local user account didn't exist in AD. That's a major security hole since hacking a local account's credential is completely undetectable. It doesn't require AD to authenticate, so AD has no idea that a brute force attack is happening."

The two month effort culminated in a report that required STEALTHbits to communicate some uncomfortable truths to the Company. "Our job was to tell them their baby was ugly," remarked Patrick Conlon, STEALTHbits Director of Professional Services. "However, the difference between this customer and most other enterprises is that they were self-aware enough to realize they were a mess. The vast majority of organizations are simply in denial."

About STEALTHbits Technologies

STEALTHbits is a data security software company. We help organizations ensure the right people have the right access to the right information. By giving our customers insight into who has access and ownership of their unstructured data, and protecting against malicious access, we reduce security risk, fulfill compliance requirements and decrease operations expense.

STEALTHbits Technologies, Inc.
200 Central Avenue
Hawthorne, NJ 07506
P: 1.201.447.9300 | F: 1.201.447.1818
sales@stealthbits.com | support@stealthbits.com
www.stealthbits.com