ỨNG DỤNG CÔNG NGHỆ DOMAIN CONTROLLER BẢO MẬT MÁY TÍNH NGƯỜI DÙNG

ThS. Nguyễn Thị Xuân

Tổ NCPT An toàn thông tin

Tóm tắt*: Các cuộc tấn công, lây nhiễm mã độc gần đây hầu hết được tin tặc khai thác lỗ hổng tiềm ẩn trên máy tính người dùng không được bảo mật. Vấn đề đặt ra đối với người quản trị là làm thế nào để bảo vệ hàng trăm máy tính người dùng trong tổ chức tránh khỏi các nguy cơ mất an ninh an toàn đó. Một công nghệ không hề mới của Microsoft nhưng ít được các doanh nghiệp Việt Nam ứng dụng đó là Domain Controller. Mô hình Domain Controller cho phép quản lý tập trung các đối tượng tham gia vào mạng, nhằm mục đích: xác thực chính xác đối tượng (computer, user); thiết lập các chính sách về bảo mật; triển khai phần mềm, bản vá lỗ hổng từ xa một cách nhanh chóng.*

1. GIỚI THIỆU

Domain (miền hay vùng) là một khái niệm quan trọng trong mạng Window, một domain là tập hợp các tài khoản người dùng (user) và tài khoản máy tính (computer) được nhóm lại với nhau để quản lý một cách tập trung, và công việc quản lý là dành cho domain controller (bộ điều khiển miền) nhằm giúp việc khai thác tài nguyên trở nên dễ dàng và bảo mật hơn.

Trong mạng ngang hàng các máy trạm có chức năng như những hệ thống độc lập và tài khoản người dùng hay gọi là tài khoản người dùng cục bộ không thể điều khiển truy cập được tài nguyên mạng, chúng chỉ truy cập và khai thác được trên máy cục bộ. Vì vậy Domain là một phát kiến được đưa ra để giải quyết các khó khăn mà mạng ngang hàng chưa làm được, nó có nhiệm vụ tập trung hóa các tài khoản người dùng và mọi công việc quản lý, thiết lập chính sách đều thông qua bộ điều khiển miền này. Điều này giúp việc quản trị dễ dàng hơn và cho phép người dùng đăng nhập từ bất kỳ máy tính tham gia mạng.

Domain cung cấp dịch vụ thẩm định (authentication) để xác định đúng đối tượng (user, computer) khi những đối tượng này tham gia vào mạng. Tức là, khi một người dùng nào đó đăng nhập vào mạng, một bộ điều khiển miền sẽ kiểm tra tính hợp lệ của username và password họ nhập vào có chính xác và khớp với dữ liệu lưu trong máy chủ hay không?

Tài nguyên trên mạng Windows được bảo vệ bởi các Danh sách điều khiển truy cập - ACL (Access Control List). Một ACL là danh sách chỉ rõ ai có quyền làm gì. Khi người dùng cố gắng truy cập tài nguyên, họ đưa ra nhận dạng của mình cho máy chủ chứa tài nguyên đó. Máy chủ sẽ kiểm tra để chắc chắn rằng nhân dạng người dùng này đã được thẩm định, sau đó tham chiếu chéo đến ACL để xem người dùng có quyền làm gì?

Mặt khác thông qua Active Directory Database người quản trị cũng có thể triển khai các ứng dụng tới các máy trạm một cách tự động và nhanh chóng.

2. CÁC KHÁI NIỆM LIÊN QUAN

a) Domain

Domain (Miền hay Vùng) trong môi trường Window là tập các tài nguyên (tập hợp các tài khoản người dùng, tài khoản máy tính,…) được nhóm lại với nhau để quản lý tập trung.

b) Domain Controller

Domain Controller là hệ thống máy chủ được thiết lập để quản lý một Domain. Một Domain có thể có nhiều Domain Controller. Một máy chủ để trở thành Domain Controller bắt buộc phải cài đặt và khởi tạo Active Directory. Domain Controller quản lý Domain của mình thông qua Active Directory đó.

c) Active Directory

Active Directory là một dịch vụ quản lý thư mục có thể chứa các thông tin về các máy tính trong mạng, người dùng mạng, máy in, ứng dụng trên mạng,.... Bằng cách lưu trữ thông tin trong một thư mục trung tâm nên tất cả các tài nguyên này đều có thể được sử dụng chung đối với tất cả mọi người ở mọi thời điểm.

Mô hình Domain (Miền) là một kiến trúc thư mục có phân cấp các tài nguyên – Active Directory – và được sử dụng bởi tất cả các hệ thống là thành viên của Miền. Các hệ thống này có thể sử dụng các tài khoản người dùng, nhóm và máy tính trong trong thư mục để bảo mật các tài nguyên của chúng. Do đó Active Directory đóng vai trò như một trung tâm lưu trữ nhận thực, cung cấp một danh sách tin cậy chỉ ra "ai là ai" trong Miền.

Bản thân Active Directory đóng vai trò là một cơ sở dữ liệu, nó chứa một danh sách các thành phần hỗ trợ, bao gồm cả các nhật ký giao dịch (transaction log) và dữ liệu hệ thống (sysvol), ở đây chứa các thông tin về kịch bản đăng nhập và chính sách nhóm. Active Directory sử dụng giao thức LDAP (Lightweight Directory Access Protocol), giao thức bảo mật Kerberos, các chu trình đồng bộ dữ liệu và dịch vụ đồng bộ file FRS (File Replication Service).

d) Các đối tượng Active Directory được sử dụng thông dụng nhất

Domain (Miền): là một đối tượng gốc có chứa các đối tượng khác trong miền.

Organizational Unit (Đơn vị tổ chức): là một đối tượng chứa (container object) được sử dụng để tạo ra các nhóm logic bao gồm các đối tượng như máy tính, người dùng, nhóm.

User (Người dùng): thể hiện là một người dùng mạng và thực hiện chức năng là dữ liệu để nhận dạng và xác thực.

Computer (Máy tính): thể hiện là một máy tính trong mạng và cung cấp tài khoản máy tính cần thiết cho hệ thống để đăng nhập vào Miền.

Group (Nhóm): một đối tượng chứa thể hiện một nhóm logic các người dùng, máy tính hoặc các nhóm khác, độc lập trong cấu trúc của Active Directory. Các nhóm có thể chứa các đối tượng từ các OU và các Miền.

Thư mục chia sẻ: cung cấp các truy nhập dựa trên Active Directory đến một thư mục chia sẻ trong một máy tính Windows.

Máy in: Cung cấp các truy nhập mạng dựa trên Active Directory đến một máy in trong một máy tính Windows.

Mỗi đối tượng Active Directory có chứa một tập hợp các thuộc tính, chính là các thông tin về đối tượng đó. Ví dụ, đối tượng người dùng sẽ có các thuộc tính mô tả tên tài khoản, mật khẩu, địa chỉ, số điện thoại,…; Một đối tượng nhóm sẽ có các thuộc tính cho biết danh sách người dùng là thành viên của nhóm đó,…

Bên cạnh các thuộc tính thuần túy thông tin, các đối tượng còn có các thuộc tính thực hiện các chức năng quản trị, ví dụ như một Danh sách kiểm soát truy nhập ACL (Access Control List) chỉ định những ai được phép truy cập đến đối tượng đó.

e) Chính sách nhóm (Group Policy)

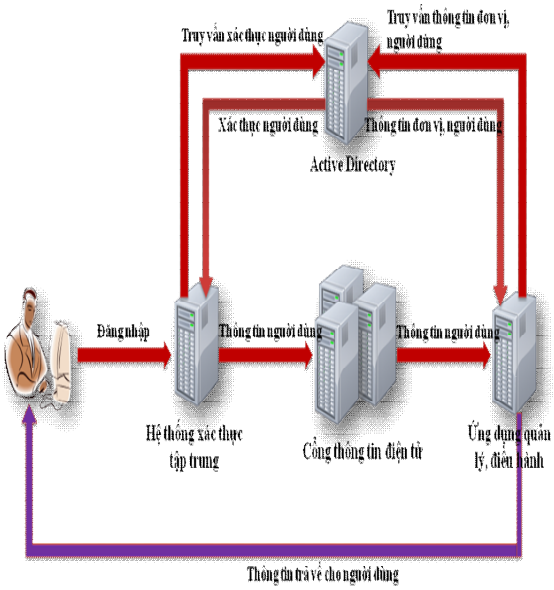
Do cách thức thừa hưởng các thiết lập từ đối tượng mức cha truyền xuống mức con, người quản trị có thể sử dụng các OU để gom các đối tượng cần cấu hình tương tự nhau. Các thiết lập cấu hình mà được áp dụng đến từng máy tính chạy Windows cũng có thể quản trị một cách tập trung nhờ sử dụng một tính năng của Active Directory gọi là chính sách nhóm (Group Policy).

Các chính sách nhóm cho phép xác định các thiết lập bảo mật, triển khai phần mềm, cấu hình hệ điều hành và cách thức hoạt động của các ứng dụng trên một máy tính mà không cần thiết phải thực hiện trực tiếp trên máy tính cần thiết lập.

Việc thiết lập các tùy chọn cấu hình trên một đối tượng đặc biệt của Active Directory gọi là đối tượng chính sách nhóm GPO (Group Policy Object) sau đó kết nối các GPO này vào các đối tượng trong Active Directory chứa các máy tính hoặc người dùng muốn áp dụng.

3. TRIỂN KHAI DOMAIN TẠI VNPT

a) Mô hình triển khai



Hình 1. Mô hình xác thực tập trung qua Active Directory

- AD (Active Directory) đóng vai trò là cơ sở dữ liệu người dùng trên mạng, cho phép kiểm tra tính hợp lệ của người dùng và lưu trữ thông tin về người dùng đó và các tài nguyên khác trên mạng.
- Hệ thống xác thực tập trung là ứng dụng trung gian, hoạt động như một dịch vụ, kiểm tra tính hợp lệ và quyền truy cập của người dùng đối với các ứng dụng và các tài nguyên trên mạng.
- Cổng thông tin điện tử đóng vai trò cổng vào tập trung, thống nhất đối với tất cả các ứng dụng, tài nguyên trên mạng.

b) Các chính sách bảo mật máy trạm

- Thiết lập các quyền truy cập tài nguyên mạng theo chức năng nhiệm vụ cho từng nhóm đối tượng.
- Các máy trạm khai thác số liệu kinh doanh chỉ được quyền sử dụng ứng dụng cho phép, không được quyền cài đặt bất kỳ phần mềm nào khác.
- Triển khai từ xa các phần mềm ứng dụng cho các máy trạm.
- Triển khai từ xa các phần mềm anti-virus cho các máy trạm, đồng thời thực hiện việc rà quét từ xa.
- Kiểm soát tình trạng kết nối của các máy trạm.
- Kiểm soát tình trạng đăng nhập, sử dụng tài nguyên của người dùng.

c) Kết quả

Domain là một khái niệm không hề mới nhưng lại ít được mô hình mạng tại Việt Nam triển khai, vì bên cạnh những ưu điểm về mặt quản lý và bảo mật thì mô hình này cũng gây không ít phiền hà, khó chịu đối với người sử dụng (do các chính sách đều bị domain controller kiểm soát).

Tuy nhiên qua quá trình triển khai thử nghiệm trên một số vùng mạng VNPT đã cho thấy những kết quả và những ưu điểm mà mô hình này đem lại:

- Việc join Domain và triển khai các chính sách an ninh cho các máy trạm khi tham gia vào mạng đã hạn chế được rất nhiều nguy cơ lây lan virus thâm nhập từ vùng mạng, các thiết bị không an toàn vào các ứng dụng chứa thông tin quan trọng của Tập đoàn.
- Việc join Domain và triển khai các ứng dụng từ xa cho các máy trạm được một cách nhanh chóng.
- Kiểm soát và phân chia đúng quyền hạn cho các nhóm đối tượng khác nhau được phép truy cập vào các nguồn tài nguyên trên mạng.

4. KẾT LUẬN

Domain là một mô hình quản lý tập trung rất hữu hiệu trên môi trường Window, giúp giảm tải công việc cho người quản trị mạng máy tính trong các vấn đề liên quan đến quản lý và bảo mật:

- Xác thực đúng đối tượng (user, computer) thông qua cơ sở dữ liệu lưu trên Active Directory. Mặt khác vì quản lý profile tài khoản người dùng tập trung trên máy chủ nên người dùng hoàn toàn có thể truy cập từ bất cứ máy tính nào trên mạng (có join domain) để làm việc với các quyền, giao diện không thay đổi.
- Thiết lập các chính sách bảo mật thông qua ACL như về: quyền truy cập, thời gian truy cập, quyền cài đặt ứng dụng lên

máy tính, quyền truy cập tài nguyên trên mạng,…

- Triển khai các ứng dụng từ xa tới các máy trạm một cách nhanh chon như các phần mềm ứng dụng, phần mềm diệt virus, các bản vá (patch) cho hệ thống.

5. TÀI LIỆU THAM KHẢO:

1. *Robbie Allen - Active Directory Cookbook, 2003.*
2. *Tài liệu nội bộ "Phương án triển khai domain cho mạng VNPT" của nhóm bảo mật CDiT.*
3. *www.quantrimang.com.vn.*

Thông tin tác giả: **Nguyễn Thị Xuân**

Năm sinh: 1979

Lý lịch khoa học:

- Tốt nghiệp Đại học Công nghệ thông tin, trường Đại học Công nghệ, Đại học Quốc gia Hà Nội năm 2001.
- Tốt nghiệp Cao học Công nghệ thông tin, trường Đại học Công nghệ, Đại học Quốc gia Hà Nội năm 2008.
- Hiện đang công tác tại tổ Nghiên cứu Phát triển An toàn thông tin thuộc Viện công nghệ Thông tin và Truyền thông – CDiT, Học viện Công nghệ Bưu chính Viễn thông.

Lĩnh vực nghiên cứu hiện nay: Tiêu chuẩn quản lý an toàn hệ thống thông tin, giải pháp và công nghệ bảo mật.

Email: xuannt@ptit.edu.vn ; xuannt@cdit.com.vn