Whitepaper: Network Access Protection

Sicherheit im Unternehmensnetzwerk

Moderne Unternehmen kommen heutzutage nicht mehr ohne ein funktionstüchtiges Netzwerk aus. Das Tagesgeschäft und die damit verbundenen Umsatze hängen direkt von den Anwendungen ab, die über das Netzwerk erreichbar sind. Das beginnt bei E-Mail, geht über Büroanwendungen wie Textverarbeitung und Tabellenkalkulation und macht auch vor der Telefonie nicht halt, welche oft genug auch bereits über eine IP-Infrastruktur läuft.

Demzufolge hängt viel von der Verfügbarkeit und Sicherheit des Firmennetzwerkes ab. Um diese zu erhöhen, werden zentrale Komponenten doppelt (redundant) ausgeführt, um im Servicefall einer der beiden Geräte immer noch Verfügbar zu haben. Ebenso werden wichtige Verbindungen gedoppelt.

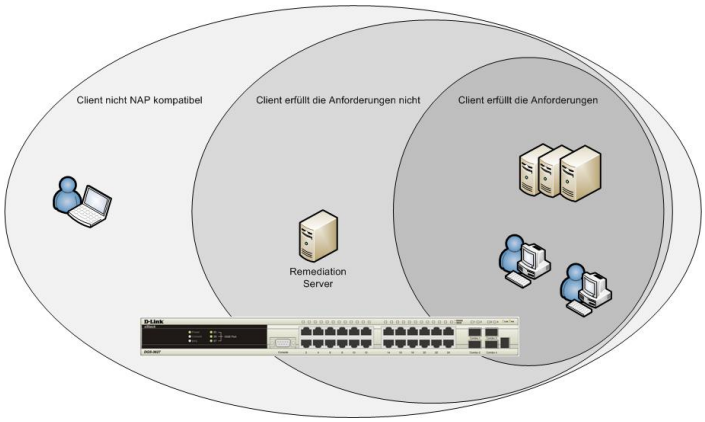
Zugriff auf Daten erhält ein Teilnehmer im Netzwerk im Normalfall über eine Domänenanmeldung an einem zentralen Serversystem. Um auch bereits den eigentlichen Zugriff auf das Netzwerk zu autorisieren, kann die Domänenanmeldung auch zur Anmeldung am Netzwerk über 802.1X realisiert werden. Hierzu müssen die D-Link Switches und auch die Clients / Server mit einer entsprechenden Konfiguration versehen werden. Ein Anwender bekommt nur dann Zugriff auf das Netzwerk und die daran angeschlossenen Ressourcen, wenn er gültige Anmeldedaten wie Username und Passwort vorweisen kann und sich mit diesen am Netzwerk über 802.1X korrekt autorisiert.

Weitergehend ist der Zugang zum Internet durch Firewalls gegen Angriffe aus dem Internet geschützt. Hier leisten Paketfilter, welche die Quell IP-Adresse, die Ziel IP-Adresse sowie den TCP-Port der einzelnen, aus dem Internet eintreffenden Pakete genauer ansehen, durchweg gute Dienste. Weiterhin kann die Ausnutzung von bekannten Sicherheitslöchern auf öffentlich zugänglichen Systemen, wie zum Beispiel Web- oder FTP-Server, durch Intrusion Prevention Systeme (IPS) verhindert werden. Diese IPS analysieren die einzelnen Datenpakete nicht nur aufgrund der IP-Adressen, sondern suchen auch gezielt nach bekannten Attacken und verhindern diese.

Die Anzahl mobiler Anwender, die sowohl innerhalb des Firmennetzes als auch außerhalb über Fremdnetze, Hotspots oder Homeoffice online gehen, ist in den letzten Jahren kontinuierlich gestiegen. Die Laptops dieser Anwender sind mitunter längere Zeit nicht am Firmennetzwerk angeschlossen. Virenscanner können veraltet sein und Patches für das Betriebssystem noch nicht implementiert sein.

Hat sich erst einmal ein Virus in einen dieser mobilen Rechner, z.B. durch einen mitgebrachten USB-Stick eingenistet, so kann sich dieser innerhalb weniger Sekunden über das gesamte interne Netzwerk verteilen und somit sehr hohen Schaden anrichten und äußert sich zum Beispiel durch einen Ausfall von Servern, Verlust von wichtigen Unternehmensdaten oder auch in Arbeitsstunden zur Wiederherstellung der Systeme. Aber nicht nur der gerne zitierte USB-Stick kann zur Verbreitung von Viren beitragen. Auch die eigenmächtige Abschaltung der Firewall durch den Mitarbeiter während eines Kundenbesuchs birgt nicht zu unterschätzende Gefahren für die Sicherheit im eigenen Firmennetzwerk.

Werden Rechner oder auch Server nicht mit den durch die Hersteller von Betriebssystemen bereitgestellten Patches versehen, so können Angreifer existierende Sicherheitslücken mehr oder weniger leicht ausnutzen, um an sicherheitsrelevante Daten (z.B. Personal- oder Angebotsdaten) zu gelangen.

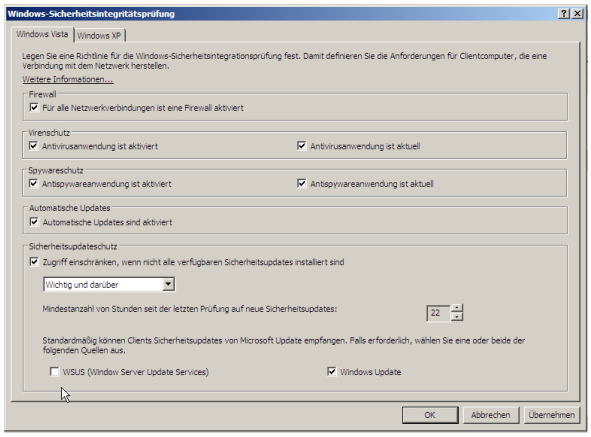


Eine Möglichkeit zur Unterbindung dieser Risiken wäre beispielsweise die Einschränkung der Nutzerrechte. Hierbei stellt sich jedoch noch kurzer Zeit das Problem, dass Anwender beispielsweise Komponenten selbst installieren müssen, um Ihre tägliche Arbeit zu erledigen. Exemplarisch kann hier die Installation von Druckertreiber genannt werden.

Die optimale Lösung

Die optimalste Lösung wäre in diesem Fall die Möglichkeit, den Client bereits vor dem Zugriff auf firmeninterne Server auf Sicherheitsrisiken hin zu überprüfen. Bestehen Risiken, kann der Zugriff durch eine Netzwerkkomponente geblockt werden, bis das Sicherheitsproblem behoben ist. Weiterhin denkbar wäre die Schaffung eines Quarantänenetzes in welchem beispielsweise der Virenscanner und die Betriebssystemdateien durch Patches aktualisiert werden können.

Whitepaper: Network Access Protection



Genau diese Anforderung kann mit Hilfe von **Network Access Protection**, kurz **NAP**, bei Microsoft basierenden Systemen realisiert werden.

Grundvoraussetzung hierfür ist auf der Seite des Servers ein Windows 2008 Serverbetriebssystem und auf der Seite des Clients entweder Windows XP (min SP 3), Windows Vista oder Windows 7. Im Bereich der Netzwerkkomponenten wird hier ein NAP-fähiger D-Link Switch oder AccessPoint benötigt.

NAP stellt hierbei eine Erweiterung auf Basis von 802.1X dar. Im Zuge der Anmeldung des Clients über 802.1X am Netzwerk wird die Sicherheit des Clients / Servers überprüft. Zwar kann NAP auch im sogenannten DHCP Mode betrieben werden. Hierbei wird aber vorausgesetzt, dass der Client sich über DHCP eine IP-Adresse zuteilen läßt. Während dieser Zuteilung kann dann über NAP die Sicherheit des Clients geprüft werden. Wurde aber eine IP-Adresse fix auf dem Clients vergeben, so bekommt dieser Zugriff auf das Netzwerk, auch wenn er die Sicherheitsrichtlinien nicht erfüllt.

Der Ablauf im Netzwerk

Die von NAP unterstützte, clientseitige Verbindung zum Firmennetzwerk kann auf verschiedene Arten geschehen. Möglich sind beispielsweise VPN Verbindungen wie PPTP oder IPSec, über ein Terminaldienste-Gateway oder Verbindungen über drahtgebundene (LAN) bzw. drahtlose (WLAN) Medien. Nach erfolgreichem Verbindungsaufbau kommunizieren der NAP Agent des Windows Client und der Windows Server bzgl. des „Gesundheitszustands" des Clients. Hieraus können folgende Ergebnisse resultieren:

1. **Der Client ist nicht NAP kompatibel**
   Eventuell ist der Windows Betriebssystem kein Windows XP (SP3), kein Windows Vista oder Windows 7. Möglich ist auch, dass der NAP Agent auf dem Client nicht gestartet wurde.

2. **Der Client erfüllt die Anforderungen nicht**
   Der Windows Client erfüllt die im Server gesetzte Anforderung nicht. Beispielsweise wurde die Firewall deaktiviert oder der Virenscanner ist inaktiv.

3. **Alle Anforderungen werden vom Client erfüllt**
   Der Windows Client erfüllt die im Server gesetzten Anforderungen. In der Praxis bedeutet dies:

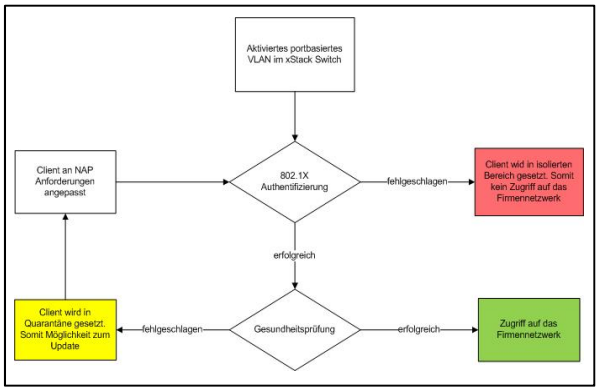
   a. *Der Virenscanner ist auf dem aktuellen Stand*
   b. *Das Betriebssystem ist auf dem neusten Stand*
   c. *Die Firewall ist aktiviert*

In Abhängigkeit des oben aufgeführten Ergebnisses sind folgende Maßnahmen des Servers möglich:

- Der Client hat keinen Zugriff auf das interne System. Er wird über den D-Link Switch/AP in ein VLAN vermittelt, welches isoliert vom internen Firmennetzwerk ist und bei dem er keinen Teilnehmer des internen Netzes erreichen kann. Die Berechtigung zur Nutzung strikt limitierter Zugriffe wie spezielle Drucker oder Zugriff über Webbrowser oder Mailprogramm auf das Internet kann im Netzwerk konfiguriert werden.

- Der Client wird einem VLAN zugewiesen indem nur ein sehr beschränkter Zugriff auf das Netzwerk möglich ist. Hierdurch besitzt er beispielsweise die Möglichkeit den Virenscanner zu aktualisieren oder das Betriebssystem auf den neusten Stand zu bringen.

- Der Client erhält uneingeschränkten Zugriff auf das VLAN des Firmennetzwerks und somit auf das komplette Firmennetzwerk.



Whitepaper: Network Access Protection

Mit Hilfe von NAP und einer hierfür geeigneten Netzwerkumgebung wie der von D-Link ist es Möglich, die Sicherheit im Netzwerk noch einmal zu erhöhen. Angriffe im Netzwerk werden vermieden und die Administratoren bekommen eine skalierbare Möglichkeit, die Sicherheitseinstellungen und Softwarepflege auf den Clients auf einem definierten Stand zu halten. Auf neue Sicherheitsrisiken kann schnell reagiert werden und die Verantwortung, dringend benötigte Patches auf ein System zu installieren, wird nicht auf den Anwender übertragen.

Mit Hilfe der Netzwerkkomponenten von D-Link ist die Unterstützung von NAP schnell eingerichtet. Zusammen mit anderen Sicherheitsfunktionen wie IP-MAC-Port Binding oder auch Loopback Detection wird so die Verfügbarkeit des Netzwerkes und der daran angeschlossenen Systeme signifikant gesteigert.

Aktuelle Themen im Rahmen Sicherheit	Stabilität	Performance	Redundanz	Verwaltbarkeit	D-Link Lösung
	Loop Connections				**Loopback–Detection**
	Mehrere DHCP Server				**DHCP Server Screening**
	Wurm Ausbrüche				**SafeguardEngine**
Wurm Ausbrüche					**Zonedefense**
ARP Spoofing					**IMPB v3**
Man in the Middle Attack					**IMPB v3**
Grundsätzlich geschützter Netzwerkzugriff					**ACL Liste Web based Access (WAC) 802.1x**
Erweiterter Netzwerkzugriff mit Policies					**Microsoft NAP**
		P2P Abusing			**Flow based Bandwidth Control**
			Chassis übergreifende Redundanz		**RERP (DES-7200)**
			Stacking		**Stacking auch über Glasfaser**
		Bandbreiten-erhöhung			**Stacking**
Überwachung / Konfigurations-rollout	Überwachung	Überwachung	Überwachung / Konfiguration	Einfache Administration	**D-View 6**

Folgende Switch Serien unterstützen NAP:

- **DGS-3400**
- **DGS-3600**
- **DES-3800**
- **DES-3526/50**
- **DES-3528/P/52**

Folgende Wireless Access Points unterstützen NAP:

- **DWL-3200AP**
- **DWL-8200AP**
- **DWL-3260AP**
- **DWL-2700AP**
- **DAP-2553**
- **DAP-2590**