Secure (RDP) Remote-Access für externe Dienstleister

Bernd KLAUS, BA
Fachhochschule Technikum
Wien, Österreich
cs20m012@technikum-wien.at

***Abstract* — Immer häufiger setzen Unternehmer auf strategische Partnerschaften bzw. externe Dienstleister. Damit einhergehend entstehen auch neue Herausforderungen für IT-Systeme. Einerseits müssen den externen Benutzern die notwendigen internen Ressourcen bereitgestellt werden, andererseits ist auf den notwendigen Datenschutz bzw. die Sicherheitsmaßnahmen zu achten. Dieses Whitepaper bietet einen Lösungsansatz zum Absichern jener Remote-Plattformen.**

Keywords* — *Remote-Access, Secure-Environment, externe Dienstleister, RDP, Citrix, Datenschutz

I. Einleitung

Dieses Dokument fokussiert sich auf die Absicherung von auf RDP sowie Citrix basierenden Umgebungen. Die grundlegende Problematik ist jene, dass in derartigen Umgebungen externe Benutzer oftmals dieselben, oder zumindest ähnliche, Zugriffe auf internen Systeme von Unternehmen erlangen wie interne Benutzer. So können Beispielsweise Benutzer-Informationen via Active-Directory ausgelesen werden, lokale Sitzungen auf dem Session-Host infiltriert werden, illegale Software ausgeführt werden oder auf nicht erlaubte Netzwerk-Ziele zugegriffen werden. Selbstverständlich stellt diese Auflistung nur einen kleinen Bereich an Möglichkeiten dar, umso wichtiger erscheint eine entsprechende Absicherung und Abschottung derartiger Systeme auf technischer sowie organisatorischer Ebene.

Im Weiteren wird der Ist-Zustand, also die Umgebung wie sie üblicherweise für Unternehmen eingesetzt wird, beschrieben. Anschließend werden einzelne Maßnahmen zur Absicherung herausgearbeitet und beschrieben, um im abschließenden Kapitel einen gewünschten Soll-Zustand zu definieren.

II. Ist-Zustand

In vielen Fällen werden keine gesonderten Maßnahmen zur Absicherung ergriffen. Eine logische Trennung der Session-Hosts erfolgt zwar durch dedizierte VMs in einer Collection, jedoch erhalten diese Maschinen identen zugriff wie VMs für interne Zwecke [1]. Auch können einige Zugriffe überhaupt nicht (ohne weiteres) verhindert werden, wie jene in das Active-Directory [2] oder auf Benutzer-Shares [3]. Welche Auswirkungen, je nach Schwachstelle, dadurch entstehen und wie dennoch eine Absicherung bewirkt werden kann wird im Kapitel Maßnahmen ausgearbeitet. Anzumerken ist jedenfalls, dass Sicherungsmaßnahmen im Regelfall gegenüber Zugriffe nur an der Perimeter-Grenze gesichert sind. Die Problematik entsteht im internen Bereich, nachdem die Benutzer authentifiziert wurden. Die Gefahr, wie sie durch interne Angriffe ausgeht, wird häufig unterschätzt [4]. Im Weiteren eine schematische Darstellung der oben beschriebenen Umgebung.

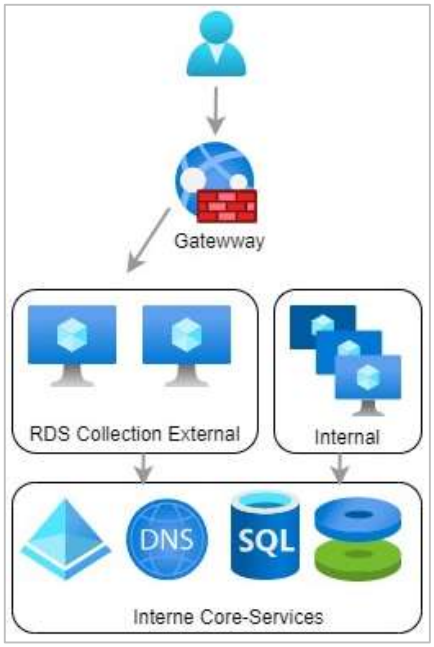

Abbildung 1: Ist-Zustand Schematisch

Weiteres Ziel ist es die Session-Hosts, welche für externe Dienstleister vorgesehen sind (siehe Grafik „RDS Collection External“) gegenüber den Core-Services abzusichern. Von einer „ausreichenden“ Abschirmung gegenüber dem Internet wird bereits ausgegangen – Firewall zwischen Internet und Gateway.

III. Sicherheitsmaßnahmen

Die Maßnahmen gliedern sich in mehrere Teile, welche unabhängig voneinander angewandt werden können. Je nach Maßnahme sind unterschiedliche Kosten sowie Aufwände verbunden. Der höchste Sicherheitsstandard wird durch die Anwendung aller angeführten Maßnahmen erreicht, dies verfolgt auch den IT-Sicherheitsgrundsatz die Absicherung in verschiedenen Schichten herzustellen („Zwiebelschalen-Prinzip“).

A. Microsoft Security-Baseline

Microsoft liefert zu jeder Betriebssystem-Version eine sogenannte „Security-Baseline“. Diese setzt sich aus einem Sammelsurium an Group-Policy-Objects (GPO) zusammen. GPOs dienen als „Konfigurations-Zentrale“ in Active-Directory gestützten Umgebungen und erlauben es nahezu jede Einstellung des Betriebssystems vorzunehmen. Die Baseline fasst dabei Einstellungen zusammen, welche zur Härtung des Betriebssystems dienen. So werden Beispielsweise alte Authentifizierungs-Methoden deaktiviert, der Device-Guard aktiviert, die Festplattenverschlüsselung konfiguriert, der Browser auf die Verwendung von neuen TLS

Versionen eingeschränkt und vieles weitere. Eine Vollständige Liste aller Einstellungen ist in Form einer Excel-Datei der Security-Baseline beigelegt. Ebenso unterstützt das Tool „Policy Analyzer“ welches Teil des „Security Compliance Toolkits“ [5] ist beim Vergleich der Einstellungen mit der aktuellen Ausprägung. Empfehlenswert ist es jedenfalls alle externen Server in eine eigens dafür vorgesehene Organization Unit (OU) zu verschieben. Das erleichtert die Handhabung und gruppiert die Server in eine logische Einheit.

Zu beachten ist, dass nach Anwendung der Security-Baseline im vollem Umfang, Single-Sign-On für Microsoft RDS-Farmen nicht mehr genutzt werden kann. Eine vergleichbare Citrix Farm ist dabei nicht betroffen. Das Problem entsteht durch die Übertragung der lokal gesicherten Anmelde-Informationen, welche eine Pass-the-Hash Attacke zulassen. So bietet Microsoft dazu zwar den Remote-Credential-Guard, welche eine sichere Übertragung der Anmeldeinformationen zu Terminal-Servern ermöglicht, jedoch nicht über ein zwischengeschaltetes Remote-Desktop-Gateway. Zum aktuellen Zeitpunkt gibt es de facto keine Lösung für diese Problematik, es steht also die Benutzerfreundlichkeit der Sicherheit des Systems gegenüber und muss individuell abgewogen werden.

Nachfolgende Grafik stellt, im Falle einer Anwendung der Microsoft Baseline-Security auf die betroffenen Server, die gewonnen Sicherheitsgewinne gegenüber Abbildung 1 schematisch dar.

Abbildung 2: Security-Baseline Hardening

B. Netzwerk Separierung

Als nächster logischer Schritt, nach der Härtung der Server selbst, ist die netzwerktechnische Verlagerung der Server in einen abgeschotteten Bereich. Dazu empfiehlt sich ein dediziertes vLAN, bzw. je nach Umgebung auch Subnetz, welches über die Firewall geroutet wird und mit entsprechenden Regel versehen wird. Grundsätzlich soll jede nicht zwingend notwendige Ziel-Adresse im internen Netz geschützt werden. Es muss also erhoben werden welche Zugriffe notwendig sind, um alle anderen Systeme zu schützen. Aus praktischen Gründen hat sich die Unterteilung in zwei unterschiedliche Gruppen an Freischaltungen herauskristallisiert, welche nachfolgend aufgelistet sind.

- **Core-Services**: Dazu zählen jene Services welche für die Nutzung der Remote-Plattform unabdingbar sind. Darunter fallen Insbesonders die folgende Zugriffe:
  - Active-Directory
  - DNS & NTP
  - Benutzer-Profil-Share
  - RDP Gateway
- **Applikationen**: jene Zugriffe, welche der Benutzer wissentlich tätigt. Dabei handelt es sich meist um Zugriffe auf Applikations-Server, Dateiablagen oder interne Web-Ressourcen wie das Intranet. Es empfiehlt sich einen Prozess für die Beantragung derartiger Freischaltung, sowie auch deren Kontrolle durch verantwortliche Personen, zu implementieren.

Zu beachten ist, dass je genauer das Regelwerk definiert wird, auch der Verwaltungs- und Wartungsaufwand entsprechend steigt. Nachfolgende Grafik veranschaulicht die durch diese Maßnahmen hervorgerufenen Änderungen gegenüber Abbildung 1.

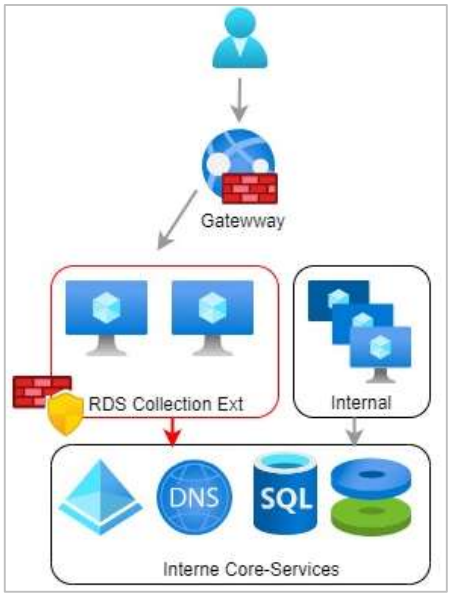

Abbildung 3: Netzwerrk-Separierung

Die offene Lücke, welche durch angewandten Maßnahmen jedoch nicht geschlossen werden kann, ist dass nach wie vor der Zugriff auf besagte Core-Services möglich und nötig sind. Ohne Beispielsweise den Zugriff auf das Active-Directory oder Benutzer-Profil-Share ist das Remote-Service schlicht nicht nutzbar. Selbstverständlich reduziert die Maßnahme die möglichen Zugriffe jedoch erheblich und kann sensible interne Systeme erfolgreich schützen.

C. Application Control

Firma Ivanti bietet mit Ihrem Produkt “Application Control” [6] einen Agent welcher es erlaubt erweiterte Sicherheits-Regeln direkt auf einzelne Benutzer anzuwenden. Die grundsätzlichen Funktionen von Applikation Control gliedert sich wie folgt:

- **Application Access Control**: einzelne Anwendungen für Benutzer erlauben oder blocken sowie das Filtern auf „trusted Owner“ oder Signaturen.
- **Network Access Control**: Granulare Steuerung für Netzwerk-Zugriffe. Für Benutzer oder Gruppen können Netzwerkzugriffe nur für eine explizit definierte Anwendung gestattet werden.
- **Analysis und Audit**: Sämtliche Vorgänge können, auch Anonymisiert, protokolliert werden.

Eine der vielfältigen Möglichkeiten, welche mit der feinen Granularität wie Application Control es bietet, ermöglicht

wird ist es: Auf ein und demselben Session-Host einen Benutzer der Gruppe „Developer“ die Anwendung VSCode.exe auf die Netzwerk-Ressource „dev.int“ zu gewähren und einem anderen Benutzer der Gruppe „Production“ die Anwendung VSCode.exe mit dem Ziel „prod.int“ freizuschalten. Wir haben also auf demselben Server, für ein und dieselbe Anwendung unterschiedliche Netzwerk-Ziele je nach Gruppenzugehörigkeit erlaubt. Allein dieses Beispiel verdeutlicht bereits die Vielfalt an möglichen Einstellungen.

Nachfolgend sind mit dieser Variante durchgeführten Änderungen schematisch dargestellt.

Abbildung 4: Application Control

Zu beachten ist, dass das Produkt von Ivanti entsprechend Lizenziert werden muss und damit auch weitere Kosten verursacht.

D. AD Object Visibility

Als letzten Schritt, welcher keinesfalls unbeachtet bleiben soll, ist es jene Zugriffe in das Active-Directory zu limitieren, bzw. die Sichtbarkeit von Objekten zu reduzieren, welche sensible Daten freigeben. Die grundlegende Problematik besteht darin, dass das Active-Directory standardmäßig von jedem Benutzer vollständig gelesen werden kann. Ein externe Benutzer kann also die Handynummer, insofern diese im AD gesichert ist, des CEOs auslesen und das ohne jegliche Hürde. Dass diese Verhalten suboptimal ist, versteht sich von selbst. Als Konsequenz daraus müssen interne Objekte entsprechend „versteckt“ werden, welches wie folgt erreicht werden kann.

Achtung: Nachfolgende Änderungen am Active-Directory können drastische Auswirkungen auf die Umgebung mit sich ziehen. Ein Backup inklusive funktionierender Restore-Routine sind absolute Voraussetzung für die Durchführung der Änderungen.

1) List Object Mode aktivieren

Um die Sichtbarkeit von Objekten sowie deren Inhalt definieren zu können ist es erforderlich den „List Object Mode“ zu aktivieren. Die Änderung betrifft den gesamten Forest und wird mittels ADSI Edit im „Configuration“ Kontext durchgeführt. Dabei wird das Attribut „dsHeuristics“ auf den Wert „001“ gesetzt. Dieses Attribut findet sich unter folgendem Pfad:

```
Services - Windows NT - Directory Service
```

2) Externe Benutzer in dedizierte OU

Als nächsten Schritt müssen alle externen Benutzer in ein eigene OU Struktur verschoben werden. Wurde Schritt A ebenfalls angewandt kann die dabei erstellte OU Struktur der Server verwendet werden.

3) Interne Benuter-OU schützen

Nun werden die internen Benutzer-Objekte, welche in der Standard-OU verblieben sind, entsprechend geschützt. Dazu wird auf der OU der Benutzer-Objekte das „List-Content“ Recht für Authentifizierte Benutzer entzogen. Ebenso wird das „List-Object“ Recht für die Benutzer auf der übergeordneten OU entfernt. Als letzter Schritt müssen alle internen Benutzer einer AD-Gruppe zugeordnet werden, welche wiederum die zuvor entzogenen Rechte erhält. Damit ist sichergestellt, dass interne Benutzer weiterhin alle Daten lesen können, externe jedoch nicht [7].

Im Anschluss sind die damit bewirkten Systemänderungen grafisch dargestellt.

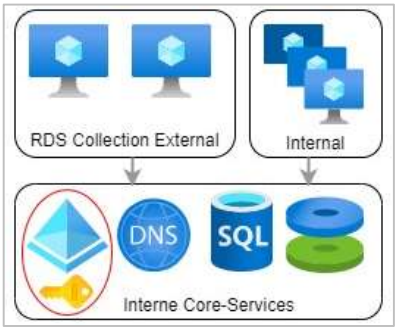

Abbildung 5: AD Object Visibility

IV. SOLL-ZUSTAND

Durch die zuvor geschilderten Maßnahmen kann die IT-Sicherheit maßgeblich gesteigert werden. Durch die Realisierung aller Punkte kann sinngemäß auch die höchste Sicherheitsstufe erreicht werden. Da dadurch jedoch hohe Kosten und Aufwände entstehen, können auch schon einzelne Maßnahme einen guten Sicherheits-Gewinn bedeuten. Dementsprechend lautet auch die Empfehlung schrittweise vorzugehen, dass vereinfacht in der Durchführung auch eine etwaige Fehlereingrenzung erheblich.

Die vollständig realisierten Maßnahmen bilden sich wie folgt ab:

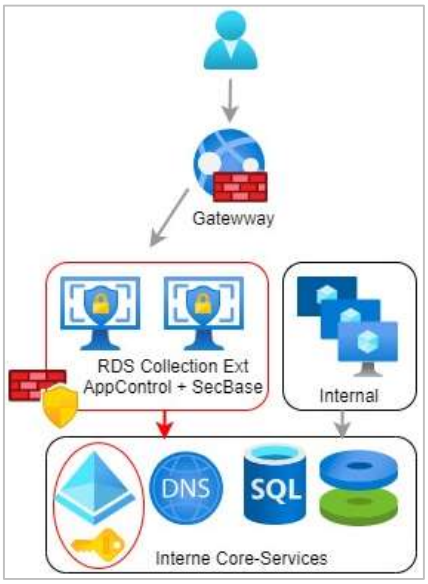

Abbildung 6: Finale Umgebung

Neben den technischen Maßnahmen müssen für einen anschließenden, sauberen Betrieb auch Regel-Prozesse etabliert werden. Je nach Variante ist ein Verantwortlicher zu definieren, welcher Freischaltungen in Form einer Genehmigungskette freigeben muss. Ebenso muss im Zuge dieser Prozesse eine saubere Dokumentation gewährleistet werden. Teilweise können die, je nach Maßnahme, Regelwerke sehr umfangreich und komplex werden.

V. DISCLAIMER

Es wird darauf hingewiesen, dass ein vollständig sicheres IT-System de facto nicht erreicht werden kann. Es verbleibt immer ein gewisses Restrisiko. Welche Maßnahmen in welchen Ausmaß notwendig sind, ergibt sich durch die wirtschaftlichen Auswirkungen wie sie im Schadenfall eintreten können. Diese gilt es individuell je Unternehmen und Branche zu beurteilen. Schlussendlich muss erwähnt werden, dass dieser Guide keinesfalls Anspruch auf Vollständigkeit erhebt. Es werden lediglich „wichtige" Hauptmaßnahmen geschildet. Gerne erweitere ich den Maßnahmen-Bereich nach Feedback.

VI. LITERATURVERZEICHNIS

[1] Microsoft Docs, „Microsoft Docs," 02 10 2017. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/desktop-hosting-logical-architecture.

[2] Microsoft Docs AD, „Microsoft Docs," 08 17 2020. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions.

[3] Microsoft Docs Permission, „Microsoft Docs," 28 06 2019. [Online]. Available: https://docs.microsoft.com/en-us/fslogix/fslogix-storage-config-ht.

[4] G. Beuster, „Thread Modelling and Risk Mitigation - An IT Security Perspective," 01 2016. [Online]. Available: https://www.researchgate.net/publication/311618130_Thread_Modelling_and_Risk_Mitigation_-_An_IT_Security_Perspective.

[5] Microsoft Docs SCP, „Microsoft Docs SCP," 21 11 2019. [Online]. Available: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10.

[6] „Ivanti Application Control," [Online]. Available: https://www.ivanti.de/products/application-control. [Zugriff am 15 03 2021].

[7] K. Bush, „Microsoft TechNet," 17 01 2015. [Online]. Available: https://social.technet.microsoft.com/wiki/contents/articles/29558.active-directory-controlling-object-visibility-list-object-mode.aspx.