2017

Kommunales Rechenzentrum
Minden-Ravensberg/Lippe

Sicherheitsrichtlinie zur Nutzung der Terminalservices

Dokumentation der ASP-Infrastruktur

ASP-Team
krz - Kommunales Rechenzentrum Minden-Ravensberg/Lippe
13.04.2017

Inhaltsverzeichnis

1. Überblick

Das krz stellt im Verbandsgebiet, in NRW und teilweise auch bundesweit Applikationen bereit, die auf Basis der Microsoft-Remotedesktopservices (RDS) und Citrix XenApp-Server betrieben und über das Citrix HDX-Protokoll zum Kunden-PC „geliefert“ werden. Um eine solche Anwendung nutzen zu können, sind einige Voraussetzungen zu erfüllen, die in diesem Dokument erläutert werden.

Als solche Voraussetzungen sind einerseits technische Voraussetzungen, wie z.B. eine aktuell zu haltende Clientsoftware von Citrix – der Citrix Receiver – zu nennen, ebenso wie aktuelle Sicherheitssoftware. Andererseits sind auch organisatorische Voraussetzungen sicherzustellen, wie z.B. dass ein Benutzerkonto nur von einer Person genutzt werden darf und dass die Kennworte unbedingt vertraulich zu halten sind.

2. Anforderungen an die Client-PCs

2.1 Vorgaben für die Client-Systemsoftware

Jeder handelsübliche Arbeitsplatz-PC ist geeignet, um eine Verbindung zu den Citrix XenApp-Servern des krz aufzubauen. Da an diesen Geräten teils vertrauliche und/oder personenbezogene Daten verarbeitet werden, müssen einige Mindestanforderungen erfüllt werden. Bitte beachten Sie, dass wir zwar unser Rechenzentrum absichern können, aber die Daten müssen auch an den Rechnern der Kunden noch sicher sein.

Für **Arbeitsplatzrechner** (**Fat Clients**) empfiehlt das krz ausdrücklich Microsoft Windows. Derzeit hat **Windows 7** die höchste Verbreitung und wird breit unterstützt, Windows 10 ist bei vielen in Vorbereitung. Nutzen Sie bitte grundsätzlich nur Windows-Versionen (egal ob Client- oder Server-Betriebssysteme), die **von Microsoft noch mit Sicherheitsupdates versorgt werden**, ansonsten können sie nicht mehr als sicher angesehen werden! Stellen Sie bitte sicher, dass Sie **keine älteren Betriebssysteme** nutzen, um auf die Verfahren des krz zuzugreifen.

Andere Betriebssysteme wie Linux oder Mac OS X sind grundsätzlich geeignet für einen Zugriff auf Citrix XenApp-Server. Da das krz solche Systeme selbst weder betreibt noch für die Verwendung empfiehlt, ist der Kunde selbst für die Funktionsfähigkeit und Aktualität des entsprechenden Citrix Receiver zuständig.

Der Zugriff über **Thin Clients** ist grundsätzlich möglich, wird vom krz aber ausdrücklich **nicht empfohlen**. Thin Clients greifen entweder über eine virtualisierte Desktop-Infrastruktur (VDI) oder kaskadiert über eine kundeneigene Terminalserver-Farm auf die Anwendungen des krz zu. Das dabei verwendete Betriebssystem muss eines der oben genannten sein.

> Die Verwendung von Thin Clients kann erfolgreich sein, birgt aber die Gefahr, durch Updates an beliebiger Stelle plötzlich auftretende, unerklärliche Probleme zu bekommen. Updates an der krz-Infrastruktur (z.B. XenServer, XenApp-Server, Webinterface, StoreFront-Server, NetScaler, Windows etc.) sind sicherheitsrelevant und gehören zum Tagesgeschäft. Daher werden Updates grundsätzlich weder angekündigt noch bekanntgegeben.
> Ausnahme: ein Produkt wird durch ein neues oder anderes ersetzt. Unabhängig davon erfolgen natürlich Informationen bei Verfahrensupdates.

Achten Sie immer darauf, dass das Betriebssystem auf einem **aktuellen Patch-Stand** ist.

2.2 Notwendige Einstellungen und Zusatzsoftware auf Seiten der Client-Arbeitsplätze

- Eine **aktuelle Anti-Viren-Software** ist aktiv.
- Die **Firewall des Betriebssystems** ist aktiv.
  Behelfsweise kann auch eine Internet Security Suite verwendet werden. Wir weisen aber darauf hin, dass dann oftmals Betriebsstörungen durch Fehlkonfiguration hervorgerufen werden können.
- Eine aktuelle Citrix-Client-Software („**Citrix Receiver**“) ist installiert.
  - Die von uns empfohlenen und unterstützten Client-Versionen für Windows stehen zum Download bereit unter **https://aspsupport.krz.de/ica-client/**.
  - Dort liegt auch eine Infodatei („**Information zur Installation.html**“), in der die aktuell empfohlene Version genannt und eine Anleitung zur Installation zur Verfügung gestellt wird. Außerdem finden sich darin Hinweise und Tipps zur Fehlersuche und -behebung.
  - Versionen für andere Betriebssysteme finden Sie unter **https://www.citrix.com/go/receiver.html**.
- Als Web-Browser kommt der **Internet Explorer** in aktueller Version zum Einsatz. Alternativ kann mit dem jeweils aktuellsten **Firefox** oder **Chrome** gearbeitet werden. Edge von Windows 10 unterstützt noch keine Erweiterungen und wird nicht sinnvoll unterstützt.
- Zertifikatsupdates für die **Stammzertifizierungsstellen** werden im Betriebssystem / im Browser automatisch aktualisiert, ggf. müssen sie nachinstalliert werden.

2.3 Der Zugriffsweg für den Anwendungsstart / Voraussetzungen im Anwendernetz

- Der Zugriff auf die vom krz bereitgestellten Anwendungen erfolgt TLS-verschlüsselt über das **Webinterface** des krz, daher muss der Anwender an seinem Arbeitsplatz HTTPS-Zugriff (Port 443) auf die Webseiten **https://cloud.krz.de/**, **https://asp.krz.de/**, **https://asp1.krz.de/** und **https://asp2.krz.de/** erhalten.
- Der Citrix Receiver bedient sich der **Internet-Verbindungseinstellungen des Betriebssystems** (= des Internet Explorers), daher sind – unabhängig vom tatsächlich verwendeten Browser – für den Internet Explorer die Proxyeinstellungen so konfiguriert, dass die oben genannten Adressen transparent ohne Einmischung eines Proxy-Servers erreichbar ist.
- **Diese Verbindung darf unter keinen Umständen vom Proxy oder der Firewall analysiert, aufgebrochen, abgehört oder auch nur z.B. per Timeout getrennt werden**.

  Wird eine Verbindung z.B. von einer **Application Firewall** überwacht, bricht diese ebenfalls den SSL-Datenstrom auf. Es ist nicht ohne weiteres möglich zu unterscheiden, ob ein solches Verhalten eine berechtigte Schutzfunktion oder eine Man-in-the-Middle-Attacke darstellt! Daher wird dies vom Citrix Receiver auf den Arbeitsplätzen und vom Citrix NetScaler als Gegenstelle für die gesicherte Verbindung nicht toleriert: **Eine solche Verbindung wird als kompromittiert angesehen und sofort getrennt**. Achten Sie daher bitte darauf, dass Verbindungen zu den oben genannten URLs transparent und ohne Trennung oder Analyse möglich sind.

2.4 Das Umfeld, in dem diesen Clients der Zugriff erlaubt ist

Der Rechner am **normalen Arbeitsplatz** befindet sich grundsätzlich innerhalb eines vom Kunden direkt gepflegten, gewarteten und überwachten Netzwerks. Systeme außerhalb dieser Netzwerke sind über VPN-Verbindungen oder ähnlich sichere Anbindungen mit dem internen Netzwerk des Kunden oder des krz verbunden.

Beim Zugang von **Telearbeitsplätzen** ist sicherzustellen, dass alle Maßnahmen für eine Sicherung des Arbeitsplatzes erfolgt sind, wie sie auch bei Arbeitsplätzen innerhalb des internen Netzwerks erfolgen müssen; ferner sollte der Zugang über **VPN-Verbindungen** erfolgen, oder mit einem Rechner, der nicht für private Zwecke vorgesehen ist.

Ein Zugriff aus **öffentlichen Netzen**, wie z.B. **WLAN-Hotspots** ist nur von entsprechend abgesicherten Rechnern und ausschließlich über VPN-Verbindungen gestattet.

Öffentlich zugängliche Rechner oder Rechner, die nicht nach den oben genannten Anforderungen gesichert sind, dürfen **nicht** für den Zugriff auf die krz-Infrastruktur und damit auch die bereitgestellten Anwendungen benutzt werden.

2.5 Grundsätzliches zur Sicherheit und den Zugangsdaten

Die Clients stellen dem Anwender eine Möglichkeit zur sofortigen Sperrung zur Verfügung (⊞-L), wenn er den Arbeitsplatz verlassen will bzw. sperren den Zugriff (z.B. nach 15 Minuten Nichtbenutzung oder Mitnahme eines Token oder einer SmartCard) automatisch.

Jeder Anwender erhält individuelle Zugangsdaten und hält diese grundsätzlich und ausnahmslos geheim. Bei gemeinsam genutzten Rechnern arbeitet trotzdem jeder Anwender nur mit seinen individuellen Zugangsdaten.

Besteht die Möglichkeit, dass die Zugangsdaten ausgespäht wurden, muss sofort mindestens das Kennwort geändert werden; bei Verdacht von zwischenzeitlichen Zugriffen durch Unbefugte ist von Kunden schnellstmöglich der Servicedesk des krz (+49 5261 252-130), von krz-Mitarbeitern der IT Sicherheitsbeauftragte zu informieren.

3. Zusätzliche Geräte, die an Clients angeschlossen werden dürfen

Allgemein bzw. je nach Verfahren werden einige Klassen von Peripheriegeräten an den Clients benötigt. Andere hingegen sind zumindest unkritisch, während es auch Geräteklassen gibt, von denen potentiell Gefahren ausgehen oder die als Sicherheitsrisiko einzustufen sind.

3.1 Für die Benutzung der krz-Anwendungen allgemein notwendige Geräteklassen

- **Bildschirme** sind selbstverständlich uneingeschränkt nutzbar. Die Mindestauflösung beträgt 1024×768 Bildpunkte, empfohlen werden mindestens 1280×1024.

  > Ein Multi-Monitorbetrieb ist grundsätzlich möglich. Man beachte jedoch, dass sich einige Anwendungen die Bildschirmeinstellungen bzw. Fensterpositionen merken und dann unter Umständen nach einer Änderung oder einem Wechsel des Arbeitsplatzes ihre Fenster in nicht sichtbaren Bereichen öffnen.

- **Eingabegeräte** (Tastaturen, Mäuse, Trackballs, externe Ziffernblöcke etc.) sind Geräteklassen, die zur Verwendung der Clientgeräte benötigt werden.

  > Beachten Sie bitte unbedingt, dass es z.B. als „Rubber Ducky“ bekannt gewordene USB-Sticks gibt, die sich als Eingabegerät am PC anmelden und dann Schadfunktionen ausführen können! Genauso gefährlich sind USB-Sticks, die sämtliche Tastatureingaben mitschneiden. Es wäre daher hilfreich, die USB-Ports außerhalb der Reichweite von Besuchern oder Kunden zu halten bzw. dafür zu sorgen, dass Unbefugte dort nichts einstecken können.

- **Smartcard-Lesegeräte** stellen eine Sonderform von Eingabegeräten dar, die in einigen Verfahren verwendet werden müssen, um Daten und Dokumente zu verschlüsseln bzw. qualifiziert zu signieren. Sie sind ggfs. für die Nutzung eines Verfahrens notwendig.

- **Drucker** (egal ob über USB, per Parallelport oder per Netzwerk mit dem Client-Arbeitsplatz verbunden) stellen grundsätzlich die einzige Möglichkeit dar, Ausdrucke aus den Verfahren auf den Citrix XenApp-Servern zu erhalten.

  > Auf den XenApp-Servern werden keinerlei Druckertreiber für Arbeitsplätze installiert, die Ausgabe erfolgt ausschließlich über den Citrix Universal Printer Driver der Citrix XenApp-Server. Printserver werden insoweit unterstützt, dass an den lokalen Arbeitsplätzen die Netzwerkdrucker angebunden werden die so an den Universal Printer Driver auf dem XenApp-Server weitergereicht werden. Auch (sauber programmierte) lokal installierte PDF- oder FAX-Druckertreiber lassen sich auf diese Weise nutzen.
  >
  > Unsauber programmierte Druckertreiber, die sich nicht an alle Vorgaben von Microsoft halten, können XenApp-Sitzungen zum Absturz bringen oder beträchtliche Störungen im Drucksystem der XenApp-Server des krz verursachen. Daher muss dafür Sorge getragen werden, dass an den Arbeitsplätzen nur von den Microsoft WHQL (Windows Hardware Quality Labs) zertifizierte Druckertreiber verwendet werden. Es ist ebenfalls unbedingt darauf zu achten, dass der Druckerhersteller den Treiber als geeignet für den Betrieb mit Citrix XenApp-Servern freigegeben hat.

- **Bilderfassungsgeräte** (Flachbettscanner, Fingerprintscanner, Unterschriftenpads etc.) können je nach Verfahren benötigt werden.

  > Für Flachbettscanner muss eine TWAIN-Schnittstelle installiert werden, da die aktuelle Schnittstelle für Bilderfassungsgeräte von Citrix XenApp-Servern über das Citrix HDX-Protokoll nur eingeschränkt nutzbar ist.

- **Netzwerkadapter** verbinden den Arbeitsplatzrechner mit dem internen Netzwerk des Kunden und sind im Normalfall im Rechner integriert, können aber auch als externe Geräte angeschlossen sein. Solche Geräte sind grundsätzlich nutzbar, egal ob sie eine kabelgebundene oder drahtlose (WLAN) Verbindung ermöglichen. Auch Verbindungen per Telefon- oder Mobilfunknetz (Modem / UMTS- / LTE-Adapter) und VPN sind möglich, näheres finden Sie unter 2.4.

- **Per Netzwerk verbundene Geräte** dürfen nur nach den oben genannten Vorgaben verwendet werden. Dabei ist es egal ob es sich um USB-Geräte, Steckkarten oder andere Formen handelt, ob sie eine Verbindung in ein LAN, WLAN, Mobilfunknetze oder VPN herstellen.

3.2 Unkritische Geräteklassen

- **USB-Hubs** sind in manchen Fällen notwendig, um die erforderliche Flut an USB-Geräten an den Endgeräten anschließen zu können (OK.EWO benötigt in Bürgerbüros Rechner mit 8 oder mehr USB-Ports).
- **Audio-Zubehör** (Soundkarten, Mikrophone, Kopfhörer/Headsets) ist ggf. beim Endanwender notwendig und stellt kein Problem dar.

  > Eine Audio-Ausgabe von über XenApp-Server bereitgestellten Inhalten **findet nicht statt**.

- **Videokameras** (meist Webcams) sind eher ungewöhnliches Zubehör für einen Arbeitsplatzrechner, sind aber ebenfalls unkritisch.

  > Eine Nutzung von am Arbeitsplatz angeschlossenen Kameras **findet** mit aktuell eingesetzten Verfahren **nicht statt**.
  >
  > Foto-Kameras werden entweder als Bilderfassungsgerät erkannt und sind als solches auch nutzbar, oder sie melden sich als Massenspeichergerät und sind in dieser Eigenschaft ein potentielles Sicherheitsrisiko (siehe unten).

- **USB-Gadgets ohne USB-Datenverbindung**, die den USB-Anschluss lediglich zur Stromversorgung nutzen, (Weihnachtsbäume, Tassenwärmer, Lämpchen, Wackeldackel, Ventilatoren, ...) erachten wir nicht als Sicherheitsrisiko im engeren Sinne.

  > Es ist aber **unbedingt zu prüfen**, ob die Geräte auch wirklich kein USB-Device im System installieren!
  >
  > Im eigenen Interesse sollten Sie darauf achten, dass die Geräte **betriebssicher** sind und auch wirklich nur die zulässige Strommenge aus dem USB-Anschluss beziehen! Geräte „ohne weitere Funktion“ dürfen ohne Anmeldung am USB-Host nur maximal 100 mA (bzw. 150 mA bei USB 3.x) verbrauchen. Wenn sie mehr Energie benötigen, müssen sie diese erst anfordern und dürfen dann bis zu 500 mA (bei USB 3.x max. 900 mA) beziehen – wenn die Anforderung allerdings fehlschlägt, müssen sie sich abschalten! Viele dieser Geräte beziehen aber ohne jegliche Anforderung 500 mA und mehr und können damit den USB-Bus und somit den Rechner oder zumindest einen aktiven USB-Hub beschädigen. Letztere sind oftmals unempfindlicher gegen solchen Missbrauch, müssen aber dann zumindest ein ausreichend starkes Netzteil haben.

3.3 Kritische Geräteklassen bzw. potentielle Sicherheitsrisiken

- **USB-Massenspeichergeräte** in jeder Form (USB-Sticks, Lesegeräte für Speicherkarten, MP3-Player, Smartphones, Tablets, Digitalkameras ohne Modus als Bilderfassungsgerät, USB-Teddybären, -Kugelschreiber, -Armbanduhren, -Taschenmesser etc.) würden beim Anschließen sofort einen Laufwerksbuchstaben erhalten. Solche Geräte sind aus manchen Programmen einer geöffneten XenApp-Sitzung erreichbar und stellen somit ein Sicherheitsrisiko dar.
- Andere Klassen von Endgeräten (nicht berücksichtigte oder neue) sind im Einzelfall zu erfragen.
- Aktuelle Entwicklungen können weitere Geräteklassen als kritisch einstufen.
  Beispiel: Umprogrammierte USB-Sticks (im Sinne von USB-Massenspeicher), die sich als Tastatur am System anmelden, um Schadcode auszuführen. Diese Art Angriff ist auch mit anderen USB-Geräten denkbar und wird bereits von Sicherheitsforschern beobachtet.