Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Grundregeln zur Absicherung von Fernwartungszugängen

Der Einsatz immer komplexerer Hard- und Software-Produkte macht es erforderlich, dass viele Nutzer zum Zwecke der Wartung oder zur Störungsbeseitigung einen Zugang von außen – d. h. in der Regel über das Internet – zu IT-Komponenten im lokalen Netz gestatten müssen. Grundsätzlich stellt die Eröffnung eines solchen Fernwartungszuganges (z. B. zu einem internen Firmen- oder Behördennetz) eine erhebliche Bedrohung dar. Selbst wenn aufwendige und wirkungsvolle Mechanismen zur Absicherung des Zuganges implementiert werden, ändert dies nichts an dem grundsätzlichen Faktum, dass durch die Fernwartungsschnittstelle für Personen außerhalb der Organisation eine direkte Zugriffsmöglichkeit auf das interne Netz sowie die darin verarbeiteten Daten eröffnet wird.

Wenn es also für eine Organisation aus wirtschaftlichen oder betriebstechnischen Gründen *zwingend notwendig* ist, das interne Netz durch eine Fernwartungsschnittstelle nach außen zu öffnen, so sollte diese zumindest bestmöglichst abgesichert werden. Ziel des vorliegenden Übersichtspapiers ist es, hierfür technische Lösungsmöglichkeiten zu skizzieren und einige grundlegende Regeln abzuleiten, die dabei zu beachten sind.

1 Heimnetze und kleinere Unternehmen

Kleine Unternehmen (z. B. Handwerksbetriebe) oder Freiberufler können es sich meist nicht leisten, zur Administration ihrer IT dauerhaft speziell geschultes Personal zu beschäftigen. Auch der Heimanwender ist mit der Konfiguration seines PCs oder der Installation spezieller Software oft überfordert. Praktisch ist es in dieser Situation, wenn man jemanden kennt, „der sich auskennt“. Auch bieten einige Internetprovider ihren Kunden Hilfe bei PC-Problemen als Service-Dienstleistung an. Unabhängig davon, ob es sich um private oder professionelle Hilfe (zumindest Unternehmen sollten Letzterer den Vorzug geben) handelt: Meist erweist es sich als zu aufwendig, dass der Experte persönlich vorbeikommt, um direkt vor Ort die Probleme zu lösen.

Produkte zum Aufbau einer Support- oder Fernwartungsschnittstelle gibt es am Markt in einer breiten Auswahl, die vom professionellen bis zum semi-professionellen bzw. privaten Bereich ein breites Spektrum an Einsatzszenarien abdeckt. Aus der Vielzahl dieses Angebotes seien hier speziell mit Blick auf eine Lösung „im kleinen Rahmen“ exemplarisch zwei Technologien kurz erläutert, welche – zumindest bei privater Nutzung – auch kostenlos zur Verfügung stehen.

Mit Hilfe der auf dem Remote Framebuffer Protocol (RFB; spezifiziert in RFC 6143) basierenden Steuerungssoftware Virtual Network Computation (VNC) ist es möglich, den Bildschirminhalt eines PC 1 (z. B. des fernzuwartenden PCs) über ein Netz (LAN oder WAN) auf den Desktop eines PC 2 (z. B. den des Fernwartungsdienstleistenden) zu über-

tragen. Der Experte an PC 2 kann also das Geschehen auf PC 1 so verfolgen, als würde er direkt auf dessen Bildschirm schauen. Die Software lässt sich dabei unterschiedlich konfigurieren: der Fernwarter kann (über Tastatur und Maus) entweder vollständigen Zugriff auf PC 1 erhalten oder seine Rechte können auf reines passives Beobachten beschränkt werden. Letzteres kann z. B. sinnvoll sein, wenn zwischen Kunden und Service parallel eine telefonische Verbindung besteht und der Experte den Anwender durch die Support-Routine leitet. Hierbei werden also auf Anweisung des Experten alle Aktionen durch den Anwender ausgeführt, wodurch dieser die volle Kontrolle über sein System behält und nichts ohne sein Einverständnis abläuft. Allerdings erweist sich dieses Vorgehen in der Praxis meist als sehr zeitraubend und umständlich, weshalb gewöhnlich dem Experten der volle Zugriff über das Wartungsobjekt zugewiesen wird. Der Anwender verfolgt dann nur visuell die Arbeiten auf seinem Rechner, kann diese jedoch jederzeit durch Beenden der Session per Mausklick abbrechen, wenn er dem Vorgehen des Experten nicht mehr vertraut.

Eine auf VNC basierende Software ist in unterschiedlicher Form bereits heute in vielen Betriebssystemen integriert (z. B. in diversen Linux-Distributionen) bzw. lässt sich auf praktisch allen Plattformen (MS Windows, diverse Unix-Derivate, Mac OS usw.) installieren. Technische Details zur Herstellung einer zu Fernwartungs- und Supportzwecken geeigneten VNC-Verbindung lassen sich im Internet finden[1]. Wem der Konfigurationsaufwand für eine VNC-Verbindung jedoch zu hoch ist, dem stehen auch alternative Remote-Control-Lösungen, wie z. B. die Produkte „Teamviewer“ oder „Netviewer“, zur Verfügung. Diese und vergleichbare Software hat den Vorteil, dass beim Aufbau der Verbindung zwischen PC 1 und PC 2 die Art, in der diese an das Internet angebunden sind, keine Rolle spielt. Der Grund hierfür ist, dass mittels der auf beiden PCs installierten proprietären Software jeweils eine Verbindung zu einem zentralen Server aufgebaut wird, der dann automatisch einen sicheren Kommunikationskanal zwischen beiden Seiten etabliert, ohne dass hierzu die jeweiligen Internet-Anbindungen umkonfiguriert werden müssen.

Dieser Vorteil wird jedoch damit erkauft, dass der Betreiber des zentralen Servers bei dieser Lösung im Prinzip auch auf die ausgetauschten Daten zugreifen kann. Insbesondere bei Fernwartungen in datenschutzrechtlich sensiblen Bereichen sollte dies berücksichtigt werden.

Unabhängig davon, für welche technische Realisierung man sich entscheidet: Ziel der bisherigen Ausführungen war es, zunächst kurz das Prinzip von Remote-Control-Lösungen zu erläutern, um nun einige grundlegende Regeln abzuleiten, wie eine solche Verbindung auch *sicher* als Fernwartungsschnittstelle genutzt werden kann.

Setzen wir also eine funktionierende Remote-Verbindung zwischen Anwender und Fernwartendem als gegeben voraus, so gilt zunächst:

Grundregel 1: Die Initiative zum Aufbau einer Support- oder Fernwartungssession muss immer vom Anwender ausgehen.

Da, wie oben bereits erwähnt, Anwender und Experte bei Fernwartungen im privaten oder semi-professionellen Bereich in der Regel parallel über Telefon miteinander kommunizieren, bietet sich dieser Weg auch für die Initiierung einer Session an: Der Anwender nimmt mit dem Fernwartenden telefonisch Kontakt auf und öffnet den Zugang von Hand. Als Alternative käme auch die Zusendung einer E-Mail mit einem Einmalpasswort in Frage, mit dem sich der Fernwartende innerhalb eines begrenzten Zeitfensters (z. B. einige Stunden) über die Remote-Control Software mit dem zu wartenden Rechner verbinden kann. Als Kommunikationsmedium zwischen Anwender und Experten kann – falls keine Telefonverbindung besteht – auch ein Chat-Programm genutzt werden, wie es in diversen Fernwartungsprogrammen bereits integriert ist.

1 Eine ausführliche technische Anleitung, wie sich mit Hilfe von Open-Source-Software eine Support-Schnittstelle für Privatnutzer und kleine Unternehmen einrichten lässt, liefert z. B. auf dem Web-Portal des Heise-Verlages der Artikel unter der URL: https://www.heise.de/ratgeber/Windows-Fernsteuerung-auf-Doppelklick-221454.html

Für die Anwendung im privaten Umfeld oder dem kleineren Unternehmen, wo lediglich Hilfe bei der Konfiguration des PCs bzw. der Fehlerbehebung benötigt wird, mögen die beiden folgenden Grundregeln nicht unbedingte Relevanz besitzen. Sobald der Fernwartende jedoch zumindest prinzipiell auch Einblick in vertrauliche Daten nehmen kann, ist zu beachten:

Grundregel 2: Die Fernwartungsverbindung sollte verschlüsselt sein.

Grundregel 3: Der Fernwartende muss sich sicher authentifizieren, bevor er Zugriff auf das System erhält.

In diversen Fernwartungsprogrammen ist eine Verschlüsselung bereits integriert. Produkte, wie z. B. VNC, bei denen dies nicht standardmäßig der Fall ist, sollten daher über einen SSH- oder VPN-Tunnel (SSH = *Secure Shell*, VPN = *Virtual Private Network*) betrieben werden. Ähnlich wie bei VNC selbst, erfordert die Einrichtung von SSH über das Internet allerdings einigen Konfigurationsaufwand, wenn die Rechner jeweils über einen Router sowie geschützt durch eine Firewall mit dem öffentlichen Netz verbunden sind[2, 3].

Die VNC-Verbindung über einen verschlüsselten Tunnel hat den Vorteil, dass nicht nur die *während* der Wartung ausgetauschten Daten für einen Angreifer weder einsehbar noch manipulierbar sind, sondern auch der User-Name und das Passwort, mit dem sich der Fernwartende *vor* Beginn der Session authentifiziert. Gemäß Grundregel 3 ist eine solche Authentifizierung grundsätzlich notwendig und in vielen VNC-Programmen auch bereits entsprechend implementiert. Ohne SSH-Tunnel gehen die Authentifizierungsdaten allerdings ggf. unverschlüsselt über das Internet und können so möglicherweise abgefangen und missbraucht werden, was dann nicht mehr als „sicher“ bezeichnet werden kann.

Mit der verschlüsselten Form des User-Namens und Passworts kann ein Angreifer in der Regel wenig anfangen, da es hieraus nicht möglich ist, auf den Klartext zurückzuschließen. Es bleibt ihm allerdings die Möglichkeit, durch eine Brute-Force Attacke, d. h. das Durchprobieren einer großen Zahl möglicher Kombinationen, die Zugangsdaten zu „erraten“. Um auch diesen Angriff auszuschließen, ist es daher sicherer, wenn sich der Fernwartende statt mit User-Namen und Passwort über ein Zertifikat authentifiziert.

2 Größere Unternehmen und Behörden

Die im letzten Abschnitt erläuterten Remote-Control-Lösungen (abgesichert durch zuverlässige Verschlüsselungs- und Authentifizierungsmechanismen) eignen sich vor allem für Szenarien, in denen ein Anwender sporadisch bei auftretenden IT-Problemen die Hilfe eines externen Experten in Anspruch nehmen möchte. Größere Organisationen (z. B. mittelständische und Großunternehmen, Behörden usw.) verfügen für solche Zwecke in der Regel hingegen über gut ausgebildetes Personal (Netz- und Systemadministratoren), welches für eine professionelle Wartung der hauseigenen IT zuständig ist. Allerdings gilt dies nur, falls die Organisation den Support ihrer IT nicht an einen externen Dienstleister ausgelagert hat. Auch setzen große Unternehmen und Behörden in der Regel sehr aufwendige Hard- und Software ein, deren Wartung ein so spezielles Know-how voraussetzt, dass diese nur vom Hersteller selbst geleistet werden kann. In beiden Fällen ist also die dauerhafte Einrichtung eines Fernwartungszugangs u. U. notwendig.

Ein wesentlicher Aspekt, in dem sich die IT einer größeren Organisation von dem im letzten Abschnitt besprochenen Szenario unterscheidet, ist die Größe und Komplexität des Netzes. Im

2 Einen kurzen Überblick, wie sich eine VNC-Verbindung über einen SSH-Tunnel einrichten lässt, gibt der Artikel „Fernzugriff auf Desktops mit VNC“ der Zeitschrift „Computerwoche“, welcher unter der URL: http://www.computerwoche.de/hardware/data-center-server/1893773/ abgerufen werden kann.

3 Auch hier bieten Remote-Control-Programme, wie Teamviewer, bei denen die Session über einen zentralen Server läuft, den Vorteil, dass die Datenverschlüsselung zwischen PC 1 und dem Server sowie zwischen Server und PC 2 unabhängig von der Art der Internet-Anbindung automatisch erfolgt. Zu beachten ist jedoch, dass hier der Schlüsselaustausch über den zentralen Server erfolgt und dessen Betreiber damit die verschlüsselten Daten - zumindest im Prinzip - auch jederzeit wieder entschlüsseln kann.

Allgemeinen besteht dieses aus einer Reihe zentraler Server mit mannigfaltigen Anwendungen (z. B. Datenbanken, Rechnungswesen, Einkauf, Vertrieb, Lagerhaltung usw.), auf die eine große Zahl von Client-Rechnern zugreifen. Eine Fernwartungssession – etwa wenn der Hersteller der Software für das Rechnungswesen ein Update einspielt – betrifft dabei meistens nur einen oder wenige der Server. Um die Integrität des restlichen Netzes durch den Fernwartungszugriff möglichst wenig zu gefährden, lautet eine weitere Grundregel daher:

Grundregel 4: Das Fernwartungsobjekt sollte – zumindest während einer Fernwartungssession – so weit als möglich vom Rest des Netzes isoliert werden, um gewollte oder ungewollte Zugriffe des Fernwartenden auf andere Rechner und Server zu verhindern. Hierzu sollte in jedem Falle mindestens eine Trennung durch Paketfilter eingesetzt werden, sodass der Fernwartungsdienstleister keinerlei Zugriff auf Rechner außerhalb der Fernwartungszone erhält.

Darüber hinaus behalten die drei bereits im letzten Abschnitt definierten Regeln natürlich weiterhin ihre Gültigkeit, d. h. der Fernwartende muss sich vor dem Aufbau einer Session – am besten durch ein Zertifikat – sicher authentifizieren und die Verbindung muss durch einen SSH- oder VPN-Tunnel verschlüsselt sein. Die technische Umsetzung dieser Maßnahmen ist hier natürlich anspruchsvoller, als im Falle der VNC-Verbindung im letzten Abschnitt.

Bevor wir darauf eingehen, formulieren wir zunächst eine weitere, damit in direktem Zusammenhang stehende

Grundregel 5: Die zur Etablierung des Fernwartungszugangs an den zentralen Sicherheits-Gateways vorzunehmenden Modifikationen sollten so gering wie möglich gehalten werden.

Simpel ausgedrückt besagt dies: Wenn man schon ein Loch in die Firewall bohren muss, sollte dieses so klein wie möglich gehalten werden. In der Praxis ist es jedoch meist nicht einfach, diese Regel optimal umzusetzen, da jede Umkonfiguration der Firewall auch stets mit der Gefahr einer Fehlkonfiguration verbunden ist. Statt nur den Zugriff auf das Wartungsobjekt freizuschalten, kann der Administrator so z. B. versehentlich das gesamte Netz öffnen und somit die zuvor im Zuge der Umsetzung von Grundregel 4 erreichte Isolierung des Wartungsobjektes wieder aushebeln. Etabliert man weiterhin die Wartungskonfiguration dauerhaft auf der Firewall, so erhöht sich die Gefahr, dass Angreifer dies ausnutzen und von außen in das Netz eindringen. Ändert man hingegen die Firewall-Konfiguration für jeden einzelnen Wartungsvorgang, so steigt mit der Zahl der Eingriffe auch das Risiko von Fehlkonfigurationen bzw. dass am Ende einer Session einfach vergessen wird, die Firewall aus dem Wartungsmodus wieder zurückzusetzen.

Um diese Gefährdungen aufgrund des direkten Durchtunnelns der Firewall zu minimieren, sollte die Verbindung über einen zwischengeschalteten Kopplungs-Server aufgebaut werden. Ähnlich wie die ebenfalls von außen zugänglichen Web-, Mail- oder FTP-Server der Organisation, befindet sich ein solcher Kopplungs-Server auch in der demilitarisierten Zone (DMZ) der Firewall. Anstelle des direkten Zugriffs auf das Wartungsobjekt im inneren Netz erhält der Fernwartende zunächst nur die Möglichkeit, einen SSH- oder VPN-Tunnel zum Kopplungs-Server aufzubauen. Erst nachdem er sich hier sicher authentifiziert hat, öffnet ein Administrator aus dem inneren Netz einen entsprechenden Tunnel vom Wartungsobjekt auf den Kopplungs-Server und etabliert damit erst eine durchgehende Verbindung zwischen Fernwartendem und Wartungsobjekt (Rendezvous Prinzip).

Da nun alle Verbindungen von außen durch die Firewall zunächst auf dem Kopplungs-Server enden, kann sich weder der Fernwartende noch ein Angreifer unerlaubten Zugriff auf das innere Netz verschaffen. Weiterhin sind auch die Forderungen nach sicherer Verschlüsselung und zuverlässiger Authentifizierung gemäß Grundregeln 2-3 technisch elegant umgesetzt. Schließlich ist auch Grundregel 1 erfüllt, da ohne aktives Zutun eines internen Administrators keine Fernwartungssession zustande kommt.

Produkte zur Realisierung einer solchen Lösung sind am Markt verfügbar.

Zum Abschluss formulieren wir noch

Grundregel 6: Die Durchführung einer Fernwartung muss protokolliert werden.

Diese Protokollierung sollte nicht nur auf dem Wartungsobjekt selbst erfolgen, sondern auch auf dem Paketfilter, der das Wartungsobjekt vom restlichen Netz isoliert sowie auf dem Kopplungs-Server. Falls ein interner Administrator die Arbeiten durchgehend überwacht, genügt es, Beginn und Abschluss der Fernwartung sowie die daran Beteiligten festzuhalten. Ist es hingegen nicht möglich, dass ein interner IT-Mitarbeiter den Fernzugriff über die gesamte Dauer der Wartung beaufsichtigt, so müssen alle Tätigkeiten protokolliert werden. Auf dem Wartungsobjekt selbst lassen sich hiermit später die durchgeführten Arbeiten im einzelnen nachvollziehen. Aus den Protokollen des Paketfilters und des Kopplungs-Servers ist ggf. ersichtlich, wenn der Fernwartende trotz aller Sicherheitsmechanismen versuchen sollte, sich unerlaubt Zugriff auf das interne Netz zu verschaffen.

3 Sicherheitsmaßnahmen in Bezug auf den Fernwartungsdienstleister

Bei den bisher beschriebenen Maßnahmen lag der Fokus stets auf dem Netz des Fernwartungskunden. Da Letzterer dem Fernwartungsdienstleister jedoch nicht nur Zugriff auf seine interne IT gewährt, sondern ihm dabei auch einen hohen Berechtigungsstatus (bis hin zu Administratoren-Rechten) einräumt, sollte der Kunde seinen Dienstleister mit großer Sorgfalt auswählen. In Bezug auf das Rechte-Management gilt dabei insbesondere folgende

Grundregel 7: Der Fernwartungsdienstleistende darf nie mehr Rechte erhalten, als er für die Erfüllung seiner Aufgaben unbedingt benötigt.

Da der Kunde keinen direkten Einfluss auf die Arbeitsweise des Dienstleisters besitzt, können sich durch dessen Nachlässigkeit oder unzuverlässiges Personal für ihn unkontrollierbare Risiken ergeben. Um diese zu minimieren, müssen daher vertragliche Vereinbarungen getroffen werden. U. a. sollten diese beinhalten:

- eine genaue Beschreibung, z. B. in Form eines IT-Sicherheitskonzepts, wie die IT-Systeme des Fernwartenden geschützt werden,
- eine genaue Festlegung der Kompetenzen und Pflichten des Wartungspersonals,
- eine Vertraulichkeitsvereinbarung,
- eine Vereinbarung, dass Daten, die während einer Wartung extern gespeichert werden mussten, sofort nach Abschluss der Arbeiten unreproduzierbar zu löschen sind.

Um über die Einhaltung dieser Pflichten auch eine gewisse Kontrolle ausüben zu können, sollte sich der Kunde vertraglich das Recht einräumen, beim Dienstleister

- Revisionen selbst durchzuführen oder durch ein hierauf spezialisiertes unabhängiges Unternehmen durchführen zu lassen.

Um die Gewissheit zu haben, dass der Dienstleister auch im Hinblick auf die Sicherheit seiner eigenen IT die wesentlichen Standards einhält, sollte der Kunde darauf achten, dass dieser

- ein Zertifikat nach ISO 27001 auf der Basis von IT-Grundschutz besitzt.

Zusammenfassend formulieren wir als letzte

Grundregel 8: Entscheidendes Kriterium bei der Auswahl des Fernwartungsdienstleisters sollte dessen Zuverlässigkeit sein. In Bezug auf diese sollte der Kunde vertraglich entsprechende Kontrollmechanismen vereinbaren.

4 Schlussbemerkung

Weitere Informationen zum Thema „Fernwartung“ finden sich auch im IT-Grundschutz-Kompendium des BSI (https://www.bsi.bund.de/IT-Grundschutz), insbesondere im Baustein OPS.1.2.5 – Fernwartung: https://www.bsi.bund.de/dok/1076616 sowie in den dazugehörigen Umsetzungshinweisen: https://www.bsi.bund.de/dok/128476

und den darin zitierten weiteren Referenzen.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.