Best-Practice-Empfehlungen für Remote Support

Der kontrollierte Zugang auf IT-Systeme, jederzeit und von jedem Ort, ist für Wartungs- und Reparaturaufgaben unverzichtbar. Allerdings werden neuerdings die Stichworte Fernzugriff und Sicherheit häufig in einem Atemzug genannt. Da werden Kassenterminals zu Malware-Opfern, fehlerhafte Konfigurationen beschwören Sicherheitsgefahren herauf und Kreditkartendaten landen in unbefugten Händen. Doch mit der richtigen IT-Managementstrategie sorgen Administratoren für klare Fernsicht auf die Informationssysteme sowie eine sichere und produktive Support-Umgebung.

Unglücksserie spektakulärer IT-Angriffe

Für viele Sicherheitsverantwortliche ist die Versuchung aktuell groß, Remote-Access-Dienste komplett zu verbieten. Hintergrund ist, dass Hacker unlängst wiederholt die Passwörter für den Fernzugriff auf POS-Terminals und IT-Systeme auskundschaften und vertrauliche Geschäftsdaten abgreifen konnten. Im Falle des US-Discounters Target erbeuteten Datendiebe auf diese Weise rund 40 Millionen Bank- und Kreditkartennummern samt der dazugehörenden PINs an den Kassen-Terminals. Der zweitgrößte Einzelhändler der USA musste einräumen, dass Informationen von rund 70 Millionen Kunden von Unbefugten ausgelesen wurden – ein geschätzter Schaden von mindestens $148 Mio.

Ebenfalls wurde ein Angriff auf das Zahlungssystem der US-Baumarktkette Home Depot bekannt, bei dem Hacker offenbar die Daten von bis zu 56 Millionen Kreditkarten erbeuteten. Allein die Kosten für die Behebung der Probleme nach dem Angriff bezifferten Sicherheitsexperten auf $62 Mio. Die Unglücksserie riss nicht ab: In einem weiteren spektakulären Fall berichtete der US-Büroausrüster Staples, dass Kassensysteme in 115 Filialen Opfer eines Cyberangriffs geworden waren und Angreifer mehrere Wochen lang umfangreiche Bestände an Kundendaten gestohlen hatten. Allen Sicherheitsvorfällen gemein war, dass Remote-Access-Zugänge als primäres Angriffsziel dienten.

Dabei stehen Remote-Access-Lösungen zur Verfügung, welche die entsprechende Sicherheit bieten. Nach wie vor sind sie ein wichtiges Werkzeug für IT-Abteilungen und Drittdienstleister, um aus der Ferne alle im Unternehmensnetz eingesetzten Lösungen zu verwalten, zu aktualisieren und Techniksupport leisten zu können. IT-Profis stehen aber immer vor der Herausforderung, wie sie die erforderlichen Management-Policies effektiv durchsetzen können. Im Unternehmensumfeld kommt es darauf an, Administratoren und Drittanbietern einen kosteneffizienten und geschützten Fernzugriff auf geschäftskritische Lösungen zu ermöglichen.

Weniger ist mehr

Die Unsicherheiten bei der Remote-Access-Nutzung beginnen damit, dass viele Unternehmen gar nicht wissen, welche Tools für den Fernzugriff auf IT-Systeme im Unternehmensnetz eingesetzt werden. Häufig finden sich für den Einzelfall benötigte Altinstallationen, die schlicht vergessen wurden, aber immer noch den Zugriff von außen ermöglichen. Die erste Best-Practice-Empfehlung zur eigenen Sicherheit im Unternehmen ist deshalb: Alle Drittanbieter und alle internen Mitarbeiter arbeiten mit der gleichen Remote-Access-Lösung.

Durch eine Konsolidierung der eingesetzten Fernzugriffswerkzeuge können IT-Verantwortliche die Kontrolle zurückgewinnen, Zugriffsrechte zentral steuern und Aktivitäten im Netzwerk überwachen. Lösungen der nächsten Generation setzen hier auf eine plattformübergreifende Konfiguration, die den Einsatz individueller Punktlösungen vermeidet. Bomgars Remote-Support-Lösung beispielsweise läuft auf allen gängigen IT-Systemen und Plattformen — von Windows-, Mac- und Linux-Rechnern bis zu Android-, BlackBerry-, iOS- und andere Mobilgeräten.

Der logisch nächste Schritt ist daraufhin, alle Kommunikationsversuche von nicht autorisierten Fernzugriffslösungen zu blockieren. Versuche, z.B. eine Direktverbindung per Remote Desktop Protocol (RDP) über Port 3389 oder per VNC über Port 590x aufzubauen, werden kategorisch gesperrt. Schließlich suchen Angreifer ganz gezielt nach Hintertüren, um an der zentralen Firmen-Firewall vorbei zu kommen — und offene Remote-Access-Ports sind eine bequeme und häufig genutzte Zugangsmöglichkeit.

Multi-Faktor-Authentifizierung und Passwortsicherheit

Zur Durchsetzung höchster Sicherheitsstandards ist eine Multi-Faktor-Authentifizierung ein unbedingtes Muss. Dabei erhalten Administratoren neben Einwahldaten einen einmalig gültigen Verifikationscode, wenn sie sich einwählen. Zur Abwehr von Brute-Force-Angriffen, die von mehreren Benutzern gemeinsam genutzte Logindaten aushebeln, empfiehlt sich die Nutzung individueller Benutzerkennungen bei der Anmeldung.

Persönliche Einwahlmöglichkeiten sind schon allein deshalb sinnvoll, weil sich ansonsten eine Protokollierung der durchgeführten Supportarbeiten nicht zuordnen lässt. Für zusätzliche Sicherheit sorgt eine zeitliche Begrenzung der Fernzugriffe. Kein Dienstleister benötigt einen 24-Stunden-Zugriff von außen an 365 Tagen im Jahr. Und noch einmal: Besonders gefährlich ist ein solcher Dauerzugang, wenn Lizenzen und Passwörter von mehreren Personen gemeinsam genutzt werden.

Apropos Passwörter: Externe Dienstleister sollten weder die gleichen Passwörter verwenden, noch sollten Sie diese Passwörter selbst kennen. Vielmehr sollte eine Passwort Vault-Lösung für die Sicherung von Passwörtern und Anmeldedaten implementiert werden. Dabei werden die Anmeldedaten für Server und andere Netzwerksysteme automatisch zur Verfügung gestellt, ohne sie dem Drittanbieter offenzulegen. Dies senkt die Erfolgsquoten versuchter Passwortangriffe erheblich.

Auditierung: Wie sind die Zugriffsrechte geregelt?

IT-Abteilungen verwenden zahlreiche Tools und Prozesse für Supportanfragen und zur Verwaltung von Benutzerrechten. Egal, ob dabei Standardsoftware oder selbst entwickelte Systeme verwendet werden – wichtig für einen reibungslosen Prozessablauf ist, dass Fernzugriffs-Lösungen eine nahtlose Integration ermöglichen. Webbasierte Remote-Access-Lösungen scheitern an dieser Vorgabe, auch wenn viele Dienstleister aus Kostengründen Web-Tools für den Zugriff auf IT-Systeme im Firmennetz nutzen.

Zu einem umfassenden Sicherheitsmanagement gehört abschließend, dass Chat-Dialoge und alle übertragenen Dateien stets mitgeschnitten werden. Nur auf Grundlage dieser Datenbasis lassen sich die intern eingesetzten IT-Systeme und Arbeitsabläufe anhand von Sicherheitskriterien analysieren und korrigieren. Einer Verizon-Studie zufolge werden viele Einbruchsversuche und Hacking-Angriffe erst nach einem Monat oder später bemerkt. Durch die Protokollierung aller Änderungen im Netzwerk lässt sich erkennen, ob unternehmensweite Sicherheitsvorgaben eingehalten wurden. Und wenn nicht, kann die IT mit den richtigen Maßnahmen wirksam gegensteuern.

Fazit: Die Sicherheit beim Einsatz von Remote-Access-Diensten basiert immer auf mehreren Faktoren. Sie beruht zum einen auf dem Einsatz der richtigen Lösung, mehr aber noch auf dem sinnvollen Zusammenspiel verschiedener Technologien. Im Rahmen einer wirksamen Sicherheitskontrolle gehört dazu, dass IT-Verantwortliche eine zentrale Benutzerverwaltung durchsetzen und Audit-fähige Protokolle abrufen können. Herkömmliche P2P-Remote-Access-Tools oder SaaS-Produkte scheitern an diesen Vorgaben, routen sensible Sitzungsdaten über Dritte und schränken die Optionen zur Integration mit internen Systemen und Verzeichnissen erheblich ein.

KONTAKT I KONTAKT@BOMGAR.COM I +49 6181 9661250 I BOMGAR.COM/DE