Heiße Nadel, kühler Kopf

Reality-Check für Remote-Access-Lösungen aus dem Feuer der Coronavirus-Pandemie

Mit Beginn der Coronavirus-Pandemie standen viele IT-Abteilungen vor der besonderen Herausforderung im Notfallmodus Möglichkeiten zu schaffen, um Mitarbeitern die Arbeit aus einem mehr oder minder improvisierten Homeoffice zu ermöglichen. Nun bietet es sich an, die Sommerphase für einen Reality-Check und eine systematische Konsolidierung zu nutzen.

Von Friedrich Wimmer, München

In der Pandemiezeit haben viele Unternehmen in kurzer Zeit umfangreiche Zugänge zu internen IT-Ressourcen aufgebaut. Bei manchen steht zu befürchten, dass dabei aufgrund der Dringlichkeit Cybersicherheitsanforderungen nicht im nötigen Umfang berücksichtigt worden sind. Nun ist es an der Zeit, eine erste Bilanz aus Sicherheitssicht zu ziehen. Es bietet sich an, die gewonnenen Erkenntnisse zu nutzen, um die nun existierenden Remote-Access-Lösungen in einen neuen Regelbetrieb zu überführen, der Cybersicherheitsanforderungen systematisch berücksichtigt.

Wege und Irrwege

Unternehmen nutzten in der ersten Phase der Corona-Pandemie eine breite Palette an Möglichkeiten, um eine produktive Arbeit ihrer Mitarbeiter aus dem Homeoffice heraus zu ermöglichen. Vor allem kamen netzwerkbasierte klassische VPN-Einwahl, Remote-Desktop-Lösungen oder cloudbasierte Collaboration-Plattformen zum Einsatz. Gemeinsam ist allen diesen Lösungen eines: Wertvolle Ressourcen werden außerhalb der physischen Grenzen der Organisation zugänglich gemacht – eine angemessene Absicherung ist also zwingend notwendig, was prinzipiell bei allen genannten Lösungen möglich ist. Natürlich spielen dabei Kriterien wie Businessakzeptanz, Kosten und auch das Know-how der IT-Abteilung eine entscheidende Rolle.

Wichtig ist vor allem, von vermeintlichen „Einfachlösungen" und Schnellschüssen auch zu Corona-Zeiten abzusehen, was während der ersten Phase der Pandemie nicht überall gelang. Corporate Trust hat in den vergangenen Wochen etliche Cybersicherheits-Vorfälle im Zusammenhang mit schlecht gesicherten Remote-Access-Lösungen aufgeklärt und als Folge davon die Wiederherstellung ganzer Netzwerke in einen vertrauenswürdigen Zustand geleitet.

Grundlegende Sicherheitsaspekte (siehe Kasten „Checkliste für Remote-Access-Lösungen") helfen dabei, die aktuell im Einsatz befindlichen Lösungen zu prüfen und abzusichern, gleichzeitig ist aber auch über eine sicherheitstechnische Weiterentwicklung des Remote-Access (RA) nachzudenken.

Erhöhte Bedrohungslage

Direkte Angriffe durch Cybercrime-Gruppierungen auf RA-Lösungen für Mitarbeiter beobachtete Corporate Trust vor allem über drei wesentliche Angriffsvektoren:

- User- und Password-Enumeration
- ungepatchte Schwachstellen in RA-Lösungen
- Wiederverwendung geleakter Zugangsdaten oder Abgreifen von Zugangsdaten über klassische Phishing-Angriffe

Darüber hinaus waren auch zweistufige Angriffe zu beobachten, wobei Angreifer aktuell offenbar zwei verschiedene Methoden präferieren:

- Ein Benutzersystem wird infiziert. Nachdem ein Benutzer mit diesem System über die RA-Lösung im Unternehmensnetzwerk eingewählt ist, erfolgt eine Infektion des Unternehmensnetzwerks.
- Eine RA-Lösung wird verwendet, um mit einem der drei oben genannten Angriffsvektoren Zugriff auf interne Ressourcen zu erhalten. Dieser Zugang dient dann in einer weiteren Angriffsstufe zur Kompromittierung anderer interner Systeme beziehungsweise dem Erlangen administrativer Rechte im Netzwerk.

Veränderte Rahmenbedingungen

Wenn ein Mitarbeiter seinen PC im Büro nutzt, sind vor dem Zugriff auf interne Ressourcen einige Sicherheitsaspekte bereits geprüft: Der Mitarbeiter ist physisch an einem bekannten Standort des Unternehmens präsent. Er hat bereits bestimmte Sicherheitskontrollen (Eingangstür, Werkstor etc.) überwunden. Zusätzlich gibt es für einen potenziellen Angreifer ein Entdeckungsrisiko durch Kollegen.

Das alles fällt beim Fernzugang weg. Dementsprechend ist die Identifikation des Mitarbeiters besonders wichtig. Sich hier allein auf ein seit Jahren veraltetes Benutzername/Passwort-Verfahren zu verlassen, ist fahrlässig. Andererseits ist auch die Benutzerfreundlichkeit im Auge zu behalten. Daher sollten Organisationen zur Sicherung die im Folgenden beschriebenen Ansätze berücksichtigen.

Systematische Bedrohungsanalyse

Für eine systematische Betrachtung der Cybersicherheitsanforderungen empfiehlt Corporate Trust einen bedrohungsbasierten Ansatz: Aus Bedrohungssicht ist dabei für Remote Access grundsätzlich ein erhöhtes Risiko aufgrund der potenziell ungesicherten Umgebung des Endpunkts/Clients festzustellen. Die zu betrachtenden Angriffsvektoren sind hauptsächlich:

- unzureichende IT-Sicherheit des verwendeten Clients
- mangelhafte Benutzerauthentifizierung
- schlechte gesicherte Übertragungswege
- Verbreitung von Schadsoftware über ungesicherte Internet-Zugangsmöglichkeiten (z. B. öffentliches WLAN am Flughafen)

Zudem spielt auch eine Rolle, gegen welche Angreiferklassen man sich verteidigen muss. Die Abwehr staatlich unterstützter Akteure, von Konkurrenzausspähung oder potenten Einzeltätern benötigt erweiterte Sicherheitsmaßnahmen. Hier sind zusätzliche Angriffsvektoren zu beachten:

- potenzieller Zugang von unbefugten Dritten zum Client
- Diebstahl / Fund von Systemen
- Abfilmen von Tastatureingaben und Bildschirm
- Ausübung von (physischem) Zwang auf Mitarbeiter

Risikobasierte Einwahl

Eine sogenannte risikobasierte Einwahl ist der Weg, der eine angemessene Sicherheit bei gleichzeitiger Benutzerfreundlichkeit verspricht. Die Basis ist eine angemessene Sicherheitsüberprüfung von Benutzer und Client sowie das konsequente Vereinfachen der Einwahl für Benutzer, solange der erkannte Risikolevel dies zulässt. Besondere Situationen erfordern hingegen besondere Maßnahmen: Beispielsweise ist bei zwei sich überlappenden Anmeldungen aus verschiedenen Ländern sofort eine Sicherheitsüberprüfung durchzuführen, bei einer Anmeldung von einem unbekannten Gerät eine zusätzliche Multi-Faktor-Authentifizierung einzufordern und

Checkliste für Remote-Access-Lösungen

_____ Extern erreichbare RA-Lösungen werden zeitnah (bestenfalls im Stundenbereich) nach Verfügbarkeit eines Sicherheitspatches oder einer Behelfslösung (Workaround) aktualisiert. Es ist organisatorisch geregelt, dass diese Sicherheitsaktualisierungen als Notfallmaßnahme gelten und nicht nur im Rahmen der normalen Wartungsfenster eingespielt werden.

_____ Die Verantwortung für die technische Sicherheit aller Teile der RA-Lösung ist klar geregelt und an kompetente Spezialisten delegiert.

_____ Es existiert ein Prozess, durch den Verantwortliche sofort über Sicherheitslücken und neue Patches wichtiger Front-Line-Systeme informiert werden.

_____ Die Authentifizierung der Benutzer erfolgt entweder risikobasiert oder ist durchgehend mit einer Multi-Faktor-Lösung umgesetzt.

_____ Es erfolgt eine angemessene Protokollierung und Überwachung aller externen Zugänge. Diese erfasst besonders auch alle Anmeldevorgänge (erfolgreich oder nicht), den Ort, von dem eine Anmeldung erfolgt, und den Sicherheitsstatus des genutzten Geräts.

_____ Die zum Zugriff auf Unternehmensressourcen benutzten Systeme werden sicherheitstechnisch kontrolliert und genügen den Securityanforderungen des Unternehmens – alternativ erfolgt die Freischaltung von Ressourcen adaptiv risikobasiert.

_____ Benutzer, die Fernzugriffe verwenden dürfen, sind bezüglich Cyberrisiken geschult. Vor allem werden neue Benutzer mit geeigneten Schulungs- und Kommunikationsmaßnahmen auf die Risiken und die Notwendigkeit ihrer Mithilfe zur Unternehmenssicherheit hingewiesen.

_____ Extern erreichbare Microsoft-Remote-Desktop-Protocol-(RDP)-Zugänge, sind unter allen Umständen zu vermeiden – auch wenn die dahinterliegenden Systeme zeitnah mit Sicherheitsaktualisierungen versorgt werden.

generell ab einem bestimmten Risikofaktor der Zugriff auf „Kronjuwelen" zu verwehren. Wird kein besonderes Risiko erkannt, genügt hingegen für die Einwahl beispielsweise die reine Bestätigung des Benutzers durch ein biometrisches Verfahren.

Checkliste für VPN-Verbindungen

_____ Es ist sichergestellt, dass ein ferngesteuertes Löschen von Daten/Systemen möglich ist.

_____ Es existiert ein etablierter Prozess, der verlorengegangene VPN-Endpoints zeitnah angemessen behandeln kann. VPN-Benutzer wissen zu jeder Zeit, an wen sie sich beim Auftreten eines möglichen Sicherheitsvorfalls wenden können.

_____ VPN-Endpoints erhalten eine eigene benutzerzentrierte zentrale (Firewall-)Konfiguration, die Zugriffe möglichst granular einschränkt und es ermöglicht, Zugriffe auf Anomalien zu überwachen beziehungsweise den aktuellen Risikostatus zu ermitteln (siehe Abschnitt „Risikobasierte Einwahl" im Haupttext).

_____ VPN-Endpoints haben eine Sicherheitskonfiguration, die den erhöhten Risiken von VPN-Benutzersystemen Rechnung trägt. Hierzu zählen allem voran eine sichere Full-Disk-Encryption, eine aktuelle Endpoint-Security-Lösung und eine angemessene Client-Firewall-Konfiguration. Ferner wird eine angemessene Bildschirm-Sperr- und Standby-Policy durchgesetzt.

_____ Sicherheitsaktualisierungen müssen auf VPN-Endpoints für alle relevanten Betriebssystem- und Softwarekomponenten zeitnah automatisch eingespielt werden, auch wenn sich sich diese längere Zeit nicht zentral einwählen.

_____ Management-, Reporting- und Monitoring-Tools für VPN-Endpoints müssen mit den zentralen Systemen kommunizieren können – zumindest sobald sich diese im Einwahlprozess befinden.

_____ Eingewählte Benutzer und ihre Geräte werden Risikoklassen zugeordnet und dementsprechend behandelt – in der Folge dieser Einstufung wird beispielsweise der Zugriff auf bestimmte IT-Ressourcen gewährt oder verweigert.

_____ Für die Einwahl oder sicherheitsrelevante Aktionen wird je nach Risikoklasse eine Multi-Faktor-Authentifizierung mit bis zu drei Methoden (z. B. Zertifikat auf dem Endgerät, Username/Passwort, Token) angefordert.

Moderne Passwortrichtlinien

Gleichzeitig sollten die Passwortrichtlinien modernisiert werden (s. a. <kes> 2020#2, S. 26). Unter anderem sind geleakte und schwache Passwörter unternehmensweit mittels Blacklists zu blockieren. Die geforderte Passwortkomplexität ist zugunsten längerer Passphrases zu reduzieren. Je nach Risiko sind für verschiedene Gruppen (z. B. Benutzer ohne Zugriff auf „Kronjuwelen" vs. Administratoren) verschiedene Passwort-Anforderungen umzusetzen. Nach dem Aufbau einer funktionierenden Cybersicherheits-Überwachung müssen Benutzer Passwörter dann nur noch ändern, wenn ein erster Hinweis auf eine Kompromittierung gefunden wurde.

Tunnelbau

Speziell für komplexere Unternehmensanwendungen ist oft ein Virtual Private Network (VPN) die einzig mögliche RA-Lösung. Bei VPN-Lösungen ist aus Sicherheitssicht vor allem die Unterscheidung zwischen Full-Tunneling- und Split-Tunneling-Modus wichtig:

Full Tunneling hat den Vorteil, dass jeglicher Internetverkehr verschlüsselt über die zentralen Systeme des Unternehmens geleitet und auf Sicherheitsverletzungen analysiert werden kann. Der Nachteil: Da jeglicher Internetverkehr über die zentralen Systeme geht, ist ein erhöhter Bedarf an Bandbreite am zentralen VPN-Gateway vorzuhalten. Ferner kann es aus Sicht des Benutzers – gerade bei Clouddiensten – aufgrund von erhöhten Latenzen zu einer langsameren Interneterfahrung kommen. Denn größere Clouddienste bieten oft die Möglichkeit, sich auf kürzestem Weg mit ihnen zu verbinden – aufgrund der Umleitung des Datenverkehrs über die Zentrale funktioniert das nicht mehr.

Vereinfacht dargestellt kann man bei vielen Unternehmen kostengünstig so lange auf eine tiefgreifende Anpassung von Sicherheitsmaßnahmen verzichten (z. B. ein eigenes Firewall-Regelwerk für VPN-Endpoints an der zentralen Firewall) wie ein VPN im Full-Tunneling-Modus zum Einsatz kommt, grundlegende Sicherheitsmaßnahmen implementiert sind und sich das Unternehmen hauptsächlich gegen breit angelegte Cyberkriminalität verteidigen möchte.

Eine **Split-Tunneling**-VPN-Lösung ist hingegen gut geeignet, um Bandbreite an zentralen Systemen zu sparen und die Nutzung von Clouddiensten zu beschleunigen. Gerade während der Corona-Pandemie ist die Verwendung dieses Modus ein beliebtes Mittel, um schnell die Performance für Benutzer zu steigern. Allerdings besteht damit das Risiko, dass der althergebrachte Schutz einer zentralen Perimeter-Firewall ohne

tiefgreifende Anpassung der Sicherheitsmaßnahmen in Teilen aufgehoben wird: Denn Angreifer können jedes kompromittierte Benutzersystem potenziell als Brücke in das Unternehmensnetzwerk nutzen, sofern eine aktive VPN-Verbindung dorthin besteht. Hinzu kommt, dass ein Angreifer „seinen" Internetverkehr an zentralen Sicherheitssystemen vorbeileiten kann.

Aufgrund der weiterhin zu erwartenden verstärkten Nachfrage nach VPN-Zugängen sowie des verstärkten Einsatzes von Clouddiensten ist es durchaus ratsam, das eigene Sicherheitskonzept und die Firewallregeln zeitnah für Split-Tunneling fit zu machen. Alternativ ist auch die Nutzung einer cloudbasierten VPN-Lösung mit eigenen Sicherheitsfunktionen denkbar. Diese bieten teilweise neue Lösungen, um die bekannten Schwächen klassischer VPN-Ansätze zu reduzieren.

In keinem Fall ist jedoch eine dauerhafte Umstellung ratsam, ohne das Sicherheitskonzept und die gesamte Sicherheitskonfiguration von Endpoints und zentralen Systemen anzupassen. Die im Kasten „Checkliste für VPN-Verbindungen" dargestellten Maßnahmen können jedoch helfen, Teile der relevanten Risiken von VPN-Clients abzumildern.

Fazit

Es gibt viele technische Optionen, wie man Benutzer befähigen kann, aus dem Homeoffice produktiv für eine Organisation zu arbeiten. Bei aller gebotenen Eile zu Anfang der Corona-Pandemie ist es spätestens jetzt an der Zeit, eine Überprüfung von im Notfallmodus eingeführten oder ausgebauten RA-Lösungen und gegebenenfalls eine nachfolgende Konsolidierung durchzuführen.

Auch wenn die empfohlenen Anpassungen für einige Unternehmen nicht unerhebliche Ressourcen erfordern, ist dies eine gute Investition in die Zukunft. Ein Großteil der benötigten Ressourcen wird dabei auf den Cybersicherheits-Monitoring-Prozess entfallen – ein effektives Sicherheitsmonitoring ist aber ohnehin auf- oder auszubauen! Um das Budget zu schonen, ist es allerdings sinnvoll, auf eine skalierbare RA-Lösung zu achten, die sich im Fortgang der Corona-Pandemie (und auch späterer Krisen) flexibel an zu erwartende Wellenbewegungen anpassen lässt. ■

Friedrich Wimmer ist Leiter IT-Forensik und Cyber-Security-Research bei der Corporate Trust Business Risk & Crisis Management GmbH.