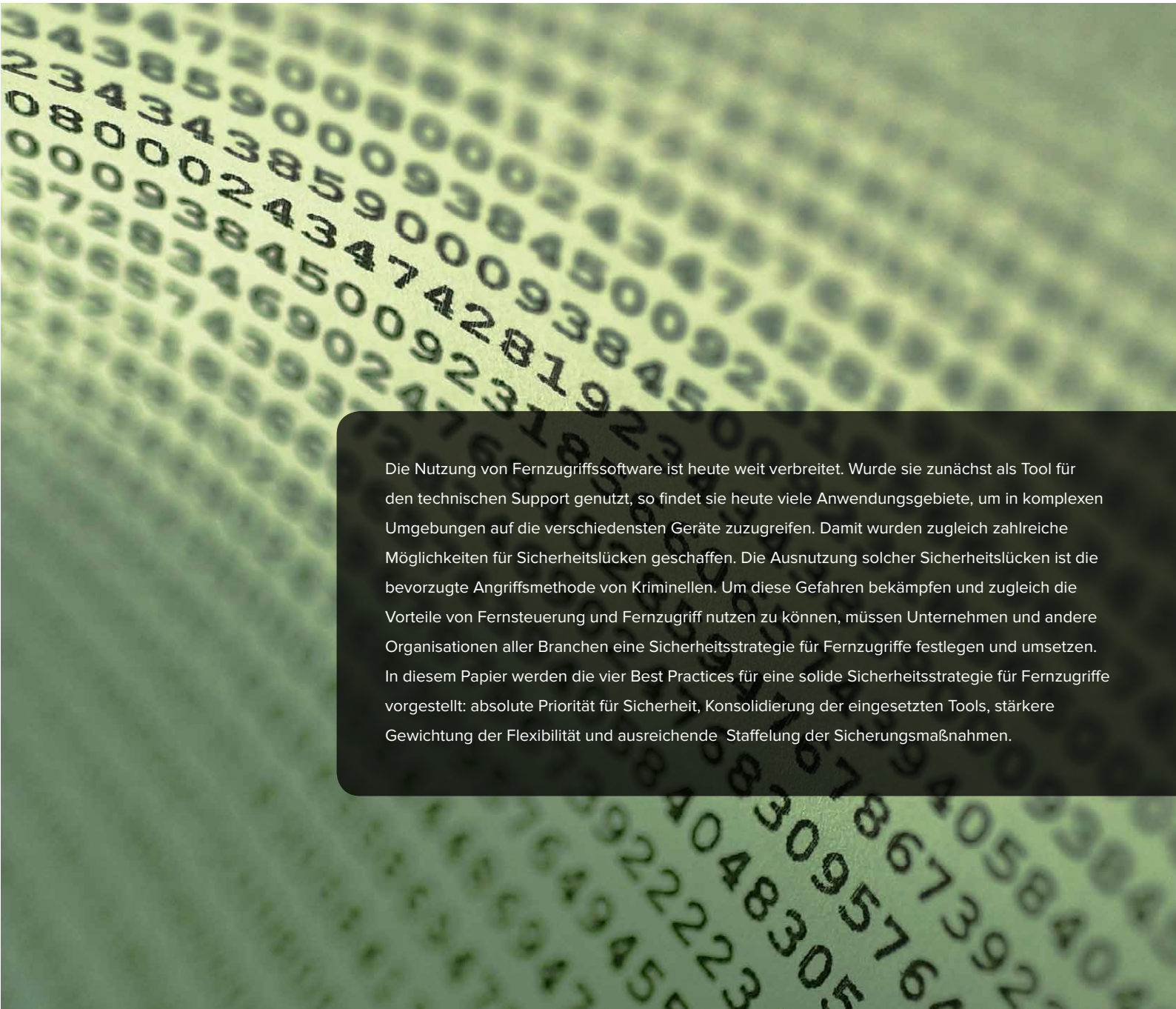
EIN WHITEPAPER VON NETOP

NETOP® Remote Control

Sicherheitsstrategie bei Fernzugriffen: Best Practices



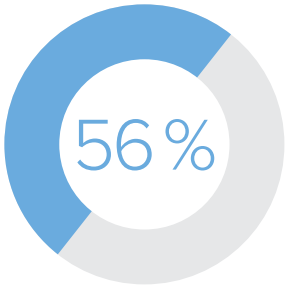
Die Nutzung von Fernzugriffssoftware ist heute weit verbreitet. Wurde sie zunächst als Tool für den technischen Support genutzt, so findet sie heute viele Anwendungsgebiete, um in komplexen Umgebungen auf die verschiedensten Geräte zuzugreifen. Damit wurden zugleich zahlreiche Möglichkeiten für Sicherheitslücken geschaffen. Die Ausnutzung solcher Sicherheitslücken ist die bevorzugte Angriffsmethode von Kriminellen. Um diese Gefahren bekämpfen und zugleich die Vorteile von Fernsteuerung und Fernzugriff nutzen zu können, müssen Unternehmen und andere Organisationen aller Branchen eine Sicherheitsstrategie für Fernzugriffe festlegen und umsetzen. In diesem Papier werden die vier Best Practices für eine solide Sicherheitsstrategie für Fernzugriffe vorgestellt: absolute Priorität für Sicherheit, Konsolidierung der eingesetzten Tools, stärkere Gewichtung der Flexibilität und ausreichende Staffelung der Sicherungsmaßnahmen.

Übersicht: Sicherheit beim Fernzugriff

Dank Fernzugriffssoftware können IT-Abteilungen Notebooks, Desktop-Computer, Server und andere Geräte miteinander verbinden, Netzwerke verwalten und technischen Support leisten. Durch Fernzugriffssoftware sparen Unternehmen Zeit, Geld und Ressourcen, da IT-Mitarbeiter wesentlich weniger unterwegs sein müssen, Ausfallszeiten verringert werden und die Effizienz der IT-Systeme verbessert wird.

Unternehmen setzen diese Technologien ein, um Abläufe zu optimieren, Kosten zu sparen, international tätig zu sein und die zunehmende Anzahl mobiler Mitarbeiter unterstützen zu können. Fernzugriffssoftware ist heutzutage nicht mehr nur ein Tool für den technischen Support, sondern integraler Bestandteil jeder IT-Infrastruktur. Kurz gesagt: Ohne Fernzugänge und Fernzugriffssoftware würden die IT-Kosten explodieren, die Zuverlässigkeit der Systeme wäre geringer und die Endnutzer wären unzufriedener.

Da sie sich bezahlt macht und das Leben erleichtert, ist Fernzugriffssoftware ein Standardtool von IT-Abteilungen. Angesichts der Bedeutung von Fernzugriffssoftware für moderne Unternehmen braucht man sich nicht darüber zu wundern, dass sich auch Kriminelle dafür interessieren. Sie versuchen gerade über Fernzugänge und Fernzugriffssoftware in Unternehmensnetzwerke einzudringen. Für fast die Hälfte aller Angriffe werden daher Fernzugänge ausgenutzt.



56 % aller Angriffe werden über Fernzugänge ausgeführt.

Datenschutzverletzungen und Computerkriminalität sind heute leider schon routinemäßige Vorfälle für Unternehmen jeder Größe und aller Branchen. Einer Untersuchung des Ponemon Institutes zufolge sind die durchschnittlichen Kosten einer Datenpanne 2015 auf 3,35 Millionen Euro gestiegen.

Die Daten von Ponemon ergeben, dass diese Kosten in den letzten beiden Jahren um 23 % gestiegen sind. Ganz gleich wie groß ein Unternehmen ist, wo es seinen Sitz hat oder in welcher Branche es tätig ist, sind die durch Datenpannen entstehenden Kosten enorm – und steigen weiter an.

Als Reaktion darauf, dass Fernzugänge und Fernzugriffssoftware zunehmend Ziel krimineller Angriffe sind, haben das FBI und das Retail Cyber Intelligence Sharing Center (RCISC) Warnhinweise und Empfehlungen für die Sicherheit von Fernzugriffen herausgegeben.

Die Empfehlungen und Anforderungen sind je nach Branche und Region etwas unterschiedlich. Standards wie der Payment Card Industry Data Security Standard (PCI DSS) gelten weltweit, während etwa die Datenschutzrichtlinie der EU (Richtlinie 94/46/EG) nur für Europa gilt. Doch ganz gleich, in welcher Branche oder Region ein Unternehmen tätig ist, kann man Eckpunkte von Sicherheitsstrategien und eine Reihe von Best Practices ausmachen, die auf praktisch alle Unternehmen und anderen Organisationen anwendbar sind.

Ganz gleich, ob Sie zum ersten Mal eine Strategie für Fernzugriffe festlegen wollen oder eine vorhandene Strategie den aktuellen Gegebenheiten anpassen möchten, sollten Sie die folgenden Best Practices berücksichtigen, um eine bestmögliche Sicherheit zu erreichen:

1. Sicherheit hat Vorrang
2. Weniger Tools
3. Flexibilität ist wichtig
4. Auf Verteidigungstiefe achten

Sicherheit hat Vorrang

Unternehmen, die ihre Strategie für IT-Sicherheit an den Zielen ihrer Gesamtstrategie ausrichten, können Risiken verringern und kurz- wie langfristig die Rentabilität verbessern. Ihr Ansatz für Fernzugriffe und deren Sicherheit sollte nur ein kleiner Teil einer umfassenden IT-Sicherheitsstrategie sein. Und diese Strategie muss unbedingt fest in die alltäglichen Geschäftsabläufe integriert werden. Sicherheit sollte nicht nur nachträglich berücksichtigt werden oder gar erst als Reaktion auf externe Bedrohung auf die Tagesordnung kommen. Sicherheit muss vorausschauend sein, eine Einstellung, mit Regeln, die zur Unternehmenskultur gehören. Auch wenn dies vielleicht wie eine große Aufgabe klingt, so sorgen die hierdurch vermiedenen Risiken und die ermöglichten Effizienzsteigerungen dafür, dass sich diese Anstrengungen auszahlen.

Der unmittelbare Nutzen einer verbesserten Sicherheit bei Fernzugriffen ist die Minimierung von Risiken. Auch wenn man den wahren Wert einer verhinderten Datenpanne kaum genau berechnen kann, so lassen sich die finanziellen Folgen von Datenverlusten leichter ausmachen. Die Untersuchung von Ponemon für 2015 ergab: „Die Durchschnittskosten für jeden verlorenen oder gestohlenen Datensatz mit sensiblen und vertraulichen Informationen haben sich von 128 Euro im letzten Jahr auf 136 Euro in diesem Jahr erhöht."

Datenpannen bedeuten nicht nur direkte finanzielle Verluste, sondern schaden auch dem Ruf eines Unternehmens. Der Verizon 2015 PCI Compliance Report besagte, dass 69 % der Verbraucher weniger geneigt sind, bei einem Unternehmen einzukaufen, das eine Datenpanne hatte. Eine umfassende Strategie für IT-Sicherheit kann die Risiken von Datenpannen wesentlich verringern und dadurch dem Unternehmen Tausende oder sogar Millionen Euro an Umsatzverlusten ersparen.

Eine umfassende IT-Sicherheit verringert nicht nur Risiken, sondern erhöht auch die kurzfristige Rentabilität. Indem Unternehmen die vorgeschlagenen Best Practices für IT-Sicherheit umsetzen, optimieren sie das Prozessmanagement und arbeiten effizienter. Wenn Sicherheitsstrategien und Unternehmensziele miteinander in Einklang gebracht werden, verringert sich auch der Verwaltungs- und Betriebsaufwand. Und bei Unternehmen, die in regulierten Branchen tätig sind, werden Überwachung und Einhaltung der Compliance ebenfalls wesentlich verbessert.

Obgleich Fernzugriffe nur einen relativ geringen Teil der gesamten IT-Infrastruktur ausmachen, haben sie eine sehr große Bedeutung für Sicherheitsrisiken und Haftungsfragen. Daher können Unternehmen ihre Risiken wesentlich verringern, wenn sie sich darauf konzentrieren, die mit Fernzugriffssoftware zusammenhängenden Bedrohungen zu bekämpfen. Investitionen in verbesserte Sicherheit bei Fernzugriffen haben ein äußerst günstiges Kosten-Nutzen-Verhältnis und machen sich daher schnell bezahlt.

ÜBER NETOP

Netop entwickelt und vertreibt marktführende Softwarelösungen, welche die schnelle, sichere und nahtlose Übertragung von Daten, Videos, Schirmbildern und Tönen zwischen mehreren Computern ermöglicht. Die von der Hälfte der Fortune 100 Unternehmen genutzten Lösungen von Netop für den sicheren Fernzugriff und Live-Chats ermöglichen es Unternehmen, besseren Kundenservice anzubieten, Supportkosten zu verringern und den Standards für Sicherheit und Compliance gerecht zu werden.

Branche der betroffenen Unternehmen

Weniger Tools

Für das Management einer zunehmend diversifizierten Infrastruktur aus verschiedenen Betriebssystemen, Softwareanwendungen, mobilen und Embedded-Geräten setzen Unternehmen nicht selten drei, vier oder fünf verschiedene Tools für Fernzugriffe ein. Leider werden gerade dadurch wesentliche Sicherheitsrisiken geradezu heraufbeschworen. Außerdem leidet die Effizienz des Betriebs darunter.

Denn wenn mehrere Produkte für Fernzugriffe eingesetzt werden, erhöht sich die Komplexität der IT-Infrastruktur. Diese erhöhte Komplexität steigert die Gefahr, sich verschiedenen Bedrohungen auszusetzen, ganz gleich wie groß das Unternehmen ist oder in welcher Branche es arbeitet. Zu diesen Bedrohungen gehören vor allem:

Verletzungen der Perimetersicherheit

Die Firewall ist meistens die erste Verteidigungslinie eines Unternehmens. Mit dem Einsatz von miteinander verbundenen Geräten in modernen Netzwerken ist es praktisch unmöglich geworden, einen einzigen Netzwerkperimeter abzusichern. Daher müssen verschiedene Sicherheitszonen mit mehreren Firewalls, DMZs, VLANs und andere Segmentierungsstrategien eingeführt werden. Für Fernzugriffe sind dann spezifische Einstellungen erforderlich, um über diese Zonen hinweg zu arbeiten. Mit mehreren Tools für Fernzugriffe benötigen Sie mehrere Konfigurationen, die verwaltet werden müssen und möglicherweise entsprechend viele Ausnahmen – oder Löcher – in Ihrer Firewall.

Anzahl der Angriffsflächen erhöht sich

Mehrere Fernzugänge und Tools für Fernzugriffe bedeuten, dass Sie Bedrohungen auch mehr Angriffsflächen bieten. Die Sicherheit der Infrastruktur lässt sich wesentlich leichter gewährleisten, wenn Sie die Anzahl Ihrer Angriffsflächen verringern. Fernzugriffssoftware, die auf bekannten Ports liegt, kann leicht von Kriminellen gescannt und zum Ziel von Angriffen gemacht werden. Wenn Sie die Anzahl der eingesetzten Tools verringern, bieten Sie weniger Angriffsflächen und behalten bei der eingesetzten Software besseren Überblick über die Sicherheit.

Fragmentierte Sicherheitskontrollen und -verfahren

Unternehmen und andere Organisationen, die Regulierungen unterliegen, müssen häufig Sicherheitskontrollen dokumentieren, um Compliance nachzuweisen. So beziehen sich die Anforderungen 7, 8, 9 und 12 von PCI DSS auf Maßnahmen zur Zugangskontrolle und Dokumentation dieser Sicherheitsrichtlinien. Mehrere Fernzugänge und Tools für Fernzugriffe bedeuten, dass diese Sicherheitskontrollen leicht fragmentiert werden. Während es noch möglich ist, die erstmaligen Kontrollen einzurichten, wird die Aufrechterhaltung dieser Kontrollen über einen längeren Zeitraum zunehmend schwieriger. Bei größeren Unternehmen wird das Change-Management durch jedes weitere Tool komplexer und schwerfälliger.

Umfassende Überwachung und Protokollierung wird erschwert

Auch wenn es keine Wunderwaffe gibt, um alle Sicherheitsprobleme zu lösen, so verbessert sich Ihre Sicherheitslage doch wesentlich durch umfassende Überwachung und Protokollierung. Eine umfassende, konsistente Protokollierung wird jedoch praktisch unmöglich gemacht, wenn mehrere Tools für Fernzugriffe eingesetzt werden, insbesondere wenn eine zentrale Übersicht fehlt. Für Unternehmen, die Regulierungen unterliegen, sind diese Möglichkeiten einer zentralen Protokollierung und Überwachung für die Compliance jedoch unentbehrlich.

Verringerte Nachhaltigkeit der Sicherheit

Angesichts der ständigen Veränderungen kann es äußerst schwierig sein, Sicherheitskontrollen über längere Zeiträume aufrechtzuerhalten. Veränderungen bei Technologien, Personal und Geschäftsabläufen haben weitreichende Auswirkungen auf die IT-Organisation. Datenpannen sind oft das Resultat krimineller Tätigkeiten, aber ergeben sich ebenfalls durch menschliche Fehler und technische Pannen. Indem Sie Fernzugriffssoftware konsolidieren und zentralisieren, verringern Sie die Möglichkeit von technischen Pannen und sorgen dafür, dass menschliche Fehler durch bessere Kontrollen aufgefangen werden können. Bei größeren Unternehmen wird die Automatisierung von Sicherheitskontrollen und Change-Management wesentlich durch eine Konsolidierung der eingesetzten Tools verbessert.

Flexibilität ist wichtig

Strategische Unternehmensziele, die auf Kostensenkungen und Effizienzsteigerungen ausgerichtet sind, stehen in einem natürliche Konflikt zu Sicherheitsstandards, welche Risiken verringern und Zugriffe beschränken sollen. Diese gegensätzlichen Zielsetzungen dann doch unter einen Hut zu bringen, erfordert sorgfältige Planung und flexible Tools.

Die Effizienz, die Sie gewinnen, indem Sie Ihre Fernzugriffssoftware konsolidieren, geht wieder verloren, wenn Sie sich für eine einzige Sicherheitslösung entscheiden müssen, die den kleinsten gemeinsamen Nenner für die Sicherheit des gesamten Unternehmens darstellt. Vorrang für die Sicherheit bedeutet nicht, in jeder Situation die höchste Sicherheitsstufe einzusetzen. Stattdessen sind Risikobewertungen erforderlich, um festzustellen, wann und wo Sicherheit benötigt wird und welche Sicherheitsstufe gerechtfertigt ist.

Sicherheit wird nicht in einer Einheitsgröße geliefert. Ihre Fernzugriffssoftware muss unterschiedliche Sicherheitsbedürfnisse für die verschiedensten Geräte, Nutzer und Netzwerksegmente ermöglichen. Flexibilität ist besonders wichtig, wenn man sich die Optionen in diesen Bereichen anschaut:

Konnektivität

Eine umfassende Fernzugriffssoftware muss Konnektivität für LAN wie Internet bieten. Bei Diensten über Internetverbindungen werden die Kontrolle und möglicherweise auch die Sicherheit verbessert, wenn Sie den Dienst selbst hosten können.

Verschlüsselung

Nicht alle Verschlüsselungsstandards und -methoden sind gleich. Finden Sie eine Lösung, die bewährte Methoden wie AES und TLS verwendet. Verschlüsselung kann auf Kosten der Systemressourcen und -effizienz gehen. Wählen Sie daher eine Lösung, die mehrere Optionen für Verschlüsselung anbietet, so dass Sie jeweils situationsabhängig das richtige Sicherheitsniveau wählen können.

Authentifizierung

Ein Auswahl an Authentifizierungsmethoden zu haben, bietet wesentlich mehr Anwendungsmöglichkeiten für Ihre Fernzugriffssoftware. Entscheiden Sie sich für eine Lösung, die Integration mit Active Directory und Multi-Faktor-Authentifizierung bietet.

Benutzerrollen und -berechtigungen

Wenn einem Benutzer sicherer Zugriff auf ein Gerät oder eine Anwendung gegeben wurde, ist es wichtig, verschiedene Optionen für Berechtigungen und Rollen zu haben. Je feiner und genauer die Berechtigungen auf die Bedürfnisse und Aufgaben der Benutzer abgestimmt werden können, desto sicherer ist das Unternehmen, ohne bei der Effizienz einzubüßen.

Protokollierung

Jedes Unternehmen hat seine eigenen Bedürfnisse hinsichtlich Protokollierung und Auditing. Während es riskant sein mag, zu viele Daten zu sammeln, kann es geradezu verheerend sein, zu wenige zu erheben. Wenn die Fernzugriffssoftware Ihnen verschiedene Optionen bietet, welche Ereignisse aufgezeichnet werden, wo und wie lange diese Protokolle gespeichert werden, können Sie die Lösung genau an die vorhandenen Bedürfnisse anpassen.

IoT NICHT VERGESSEN

Wenn Sie ihre Tools für Fernzugriffe konsolidieren, sollten Sie über die herkömmliche Tätigkeit des IT-Helpdesks hinausdenken. Eine Segmentierung Ihres Netzwerks, um den Sicherheitsanforderungen gerecht zu werden, bedeutet nicht, dass Sie auch unterschiedliche Tools einsetzen müssten. Die durch Konsolidierung gewonnene Effizienz nimmt in dem Maße zu, wie die Anzahl der eingesetzten Tools verringert wird. Achten Sie darauf, Ihre gesamte physische und virtuelle Infrastruktur zu berücksichtigen und finden Sie eine Lösung, die sowohl herkömmliche Computer, mobile Geräte, Embedded-Geräte und die zunehmend genutzten Geräte für das IoT (Internet of Things - Internet der Dinge) unterstützen kann.

Auf Verteidigungstiefe achten

Passwörter können gestohlen werden. Verschlüsselung kann geknackt werden. Systeme können und werden Gefahren ausgeliefert sein. Perfekte Sicherheit gibt es nicht. Glücklicherweise braucht sie auch nicht perfekt zu sein, um Kriminelle und Hacker davon abzuhalten, in Ihr Netzwerk einzudringen. Indem Sie Ihre Verteidigung staffeln, können Unzulänglichkeiten in einem Bereich von einem anderen abgefangen werden. Je mehr Schichten Sie anlegen, desto mehr Schutz haben Sie. Verteidigungstiefe ist ein bekannter Ansatz für IT-Sicherheit, der sich als vorteilhaft erwiesen hat.

Tiefe der Sicherung bei Ihrer Strategie für Fernzugriffe bedeutet, dass Sie Software wählen sollten, die Möglichkeiten bietet, welche über gute Verschlüsselung und starke Passwörter hinausgehen. Suchen Sie eine Lösung, die Folgendes bietet:

BEKANNTE BEDROHUNGEN VERMEIDEN

Wenn Sie sich überlegen, welche Tools Sie als Teil Ihrer Verteidigungsstrategie einsetzen, müssen Sie darauf achten, ob es bekannte Bedrohungen gibt. Viele Fernzugriffsanwendungen haben dokumentierte Sicherheitslücken mit veröffentlichten Exploits. Beliebte Fernzugriffssoftware wie Microsoft RDP oder das Open-Source-Tool VNC können sich für einzelne Bereiche Ihres Unternehmens eignen. Aber sie sind wahrscheinlich unzureichend für bestimmte Geräte oder Benutzer, bei denen erhöhte Sicherheitsanforderungen gestellt werden. Andere beliebte Produkte wie pcAnywhere, LogMeIn Pro und Teamviewer wiesen in den letzten Jahren veröffentlichte Sicherheitslücken auf. Obgleich natürlich kein Anbieter hundertprozentige Sicherheit versprechen kann, sollte die Fernzugriffssoftware (und deren Anbieter) Sie dabei unterstützen, Ihre Angriffsfläche zu reduzieren und sie nicht noch vergrößern.

Überprüfung von MAC-/IP-Adressen

Das Zielgerät akzeptiert nur Einladungen von einem Remote-User, dessen Adresse in einer festgelegten Liste von MAC-/IP-Adressen enthalten ist. Dies bietet eine grundlegende Sicherheit. Da allerdings IP-Adressen gefälscht werden können, darf dieses Merkmal nie als einzige Sicherheitsmaßnahme verwendet werden.

Geschlossene Benutzergruppen

Weisen Sie allen Benutzern und Zielgeräten Seriennummern zu, so dass sich nur die passenden Nummern miteinander verbinden können. Benutzermodule mit anderen Seriennummern werden abgewiesen. Dies ist ein Schritt in Richtung Best-in-Class-Sicherheit.

Authentifizierung

Die Fernzugriffssoftware muss sich in die Authentifizierungsmethoden integrieren lassen, die Sie gegenwärtig in Ihrem Netzwerk verwenden – ganz gleich ob es Windows Domain, LDAP-Server oder RSA SecurID-Server ist. Eine solche Integration in eine vorhandene Authentifizierungsmethode bietet eine sichere Möglichkeit für den Remote-User, sich gegenüber dem Zielgerät zu identifizieren. Für Unternehmen, die Regulierungen (wie PCI DSS) unterliegen, müssen Optionen für Multi-Faktor-Authentifizierung verfügbar sein.

Benutzergesteuerten Zugriff

Bei dieser Funktion erscheint auf dem Zielgerät eine Mitteilung, die den Endbenutzer fragt, ob er eine eingehende Anfrage von einem Remote-User akzeptiert. Erst wenn dies bejaht wird, kann die Remote-Verbindung aufgebaut werden. Dies ist eine wirkungsvolle Sicherheitsmaßnahme, die typischerweise für technischen Support eingesetzt wird.

Zusammenfassung

Die Nutzung von Fernzugriffssoftware ist heute weit verbreitet. Wurde sie zunächst als Tool für den technischen Support genutzt, so findet sie heute viele Anwendungsgebiete, um auf die verschiedensten Geräte in komplexen Umgebungen zuzugreifen. Damit wurden zugleich zahlreiche Sicherheitslücken geschaffen. Die Ausnutzung solcher Sicherheitslücken ist die bevorzugte Angriffsmethode von Kriminellen. Um diese Gefahren bekämpfen und zugleich die Vorteile von Fernsteuerung und Fernzugriff nutzen zu können, müssen Unternehmen und andere Organisationen aller Branchen eine Sicherheitsstrategie für Fernzugriffe festlegen und umsetzen. Unternehmen sollten die vier Best Practices für eine solide Sicherheitsstrategie für Fernzugriffe beachten: absolute Priorität für Sicherheit, Konsolidierung der eingesetzten Tools, stärkere Gewichtung der Flexibilität und ausreichende Staffelung der Sicherungsmaßnahmen.

Über NETOP

Netop entwickelt und vertreibt marktführende Softwarelösungen, welche die schnelle, sichere und nahtlose Übertragung von Daten, Videos, Schirmbildern und Tönen zwischen mehreren Computern ermöglicht. Die von der Hälfte der Fortune 100 Unternehmen genutzten Lösungen von Netop für den sicheren Fernzugriff und Live-Chats ermöglichen es Unternehmen, besseren Kundenservice anzubieten, Supportkosten zu verringern und den Standards für Sicherheit und Compliance gerecht zu werden. Netop ist auch Weltmarktführer bei Schulverwaltungssoftware, die Lehrer in über 75 Ländern dabei unterstützt Technologien wirkungsvoller im Unterricht einzusetzen.

Netop hat seinen Hauptsitz in Dänemark und Niederlassungen in den USA, Großbritannien, China, Rumänien und der Schweiz. Das Unternehmen vertreibt seine Lösungen direkt und über offizielle Netop Partner an Privatunternehmen und Behörden in über 80 Ländern.

Weitere Informationen unter: www.netop.com

Nachweise

2015 Cost of Data Breach Study: Global Analysis. (27. Mai 2015). Ponemon Institute, LLC. Abgerufen von: http://www-03.ibm.com/security/data-breach

2015 Trustwave Global Security Report. (9. Juni 2015) Trustwave. Abgerufen von: https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf

Empfehlungen und Warnungen: Securing Merchant Card Payment Systems from the Risks of Remote Access. (7. Juli 2015). Financial Services Sharing and Analysis Center. Abgerufen von: https://www.fsisac.com/article/alert-securing-merchant-card-payment-systems-risks-remote-access

Internet of Things Poses Opportunities for Cyber Crime. (10. September 2015). Federal Bureau of Investigation. Abgerufen von: https://www.ic3.gov/media/2015/150910.aspx

M-Trends 2015: A View from the Front Lines. (24. Februar 2015). Mandiant, a FireEye Company. Abgerufen von: https://www2.fireeye.com/WEB-2015RPTM-Trends.html

Payment Card Industry Data Security Standard version 3.1. (2015, April)

Verizon 2015 PCI Compliance Report: Insight for helping businesses manage risk through payment security. (24. März 2015). Verizon. Abgerufen von: http://www.verizonenterprise.com/pcireport/2015/

Quelle: Statista GmbH. Die Statista GmbH betreibt mit Statista.com eines der weltweit führenden Statistik-Portale. Sie hat ihren Sitz in Hamburg, Berlin, Frankfurt, New York, London und Madrid (ab 2016).