

TIPPS VON FORTINET

Checkliste für SD-WAN-Verantwortliche

7 Erfolgsfaktoren für eine sichere SD-WAN-Implementierung



Der Begriff „Software-Defined Wide Area Network“ – kurz „SD-WAN“ – mag nach einer Aufgabe für Technologie-Experten klingen. Tatsächlich aber geht das, was ein SD-WAN für ein Unternehmen bringt, weit über die Grenzen der Netzwerk-Technik hinaus. Daher ist es immer von Vorteil, wenn auch das leitende Management mit den Möglichkeiten einer SD-WAN-Implementierung vertraut ist, zumal sich hierdurch neue Perspektiven für digitale Innovationen eröffnen. Aber auch die Risiken sollten bekannt sein: Mit einem SD-WAN ergeben sich leider auch neue Gefahren durch Cyber-Kriminelle, die sich Zugang zu kritischen IT-Systemen verschaffen. Damit aus einer vielversprechenden Chance keine Datenpanne wird, sollten die folgenden sieben Faktoren berücksichtigt werden.

1. Keine Alleingänge

Zwei Drittel der Transformationsprojekte verzögern sich erheblich oder scheitern komplett am Widerstand interner Interessengruppen – wie McKinsey schon vor fast einem Jahrzehnt feststellte.¹ Das SD-WAN macht da keine Ausnahme, zumal immer mehr Menschen auf SaaS-Anwendungen wie Office 365, Google Docs oder Salesforce zugreifen und Telefonkonferenz-Software oder Dateiübertragungs-Plattformen wie Dropbox nutzen. Bevor Sie dieses funktionierende System mit einer Innovation „durcheinander bringen“, sollten Sie wichtige Interessengruppen einbeziehen, um Feedback bitten und alle Transformationsentscheidungen anhand dieser Rückmeldungen regelmäßig neu bewerten.

2. Klare, konkrete Ziele

Digitale Innovationen und ein SD-WAN sind für sich genommen keine Ziele, sondern Werkzeuge, die die Unternehmensstrategie voranbringen und selbst durch konkrete Geschäftsziele unterstützt werden. SD-WAN-Projekte, bei denen dies vorab klar kommuniziert wird, sind eher erfolgreich. Formulieren Sie strategiebezogene Ziele: Definieren Sie z. B., welche Anwendung am stärksten zu welchem Produktivitätsziel beiträgt, oder gegen welche wichtigen gesetzlichen Vorschriften bei einer Datenpanne verstoßen werden würde. Dieser Ansatz hat den Vorteil, dass die Geschäftsagenda im Mittelpunkt der SD-WAN-Implementierung steht. Sind sich alle bewusst, warum diese Umstellung notwendig ist, bleibt das Vorgehen fokussiert und das Engagement steigt erheblich.

Hauptpunkte

- Eine SD-WAN-Implementierung erfordert die Federführung durch das leitende Management, da sich dieses Vorhaben auf wichtige Geschäftsaspekte wie die Anwendungspriorisierung oder die Security-Strategie auswirkt.
- Interne Interessengruppen müssen einbezogen werden. Viele digitale Innovationen scheitern am Widerstand interner Anwender, die am Projekt überhaupt nicht beteiligt waren.
- Die Sicherheit muss im Mittelpunkt stehen. Schon in der Konzept- und Testphase sollte eine Lösung gewählt werden, die die Gesamtleistung vorhandener Security- und Netzwerk-Systeme marginal beeinflusst.
- Unabhängige Quellen sind immer eine interessante Lektüre. Unvoreingenommene Ansichten neutraler Dritter sind extrem hilfreich, wenn eine umfassende, integrierte und automatisierte SD-WAN-Lösung implementiert werden soll.

3. Automatisierungen nutzen

Obwohl jede SD-WAN-Lösung die Priorisierung von Anwendungen und VPNs unterstützt, gibt es große Unterschiede bei der Zero-Touch-Bereitstellung. In dem Moment, in dem Sie bei der SD-WAN-Implementierung an Remote-Standorten damit beginnen, die Regeln manuell zu kaskadieren oder zu ändern, sind menschliche Fehler, Verzögerungen – oder eine unvorhersehbare Kombination aus beidem – unvermeidlich. Daher sollten Sie sicherstellen, dass Ihre SD-WAN-Lösung per Automatisierung implementiert werden kann, um erhebliche Verzögerungen und Mehrkosten zu vermeiden.

4. Federführung bei Performance-Tests mit

allen aktivierten Sicherheitsfunktionen Bei Performance-Tests sind Führungskräfte auf Operations-Teams angewiesen, die diese Aufgabe häufig an externe Integratoren oder Drittanbieter delegieren. An einer Delegation ist nichts auszusetzen. Allerdings kann die SD-WAN-Leistung nach dem Aktivieren erweiterter Sicherheitsfunktionen erheblich variieren, was in den Datenblättern der meisten Anbieter oft verschwiegen wird. Das Beharren der Geschäftsleitung auf Performance-Tests unter besonderer Berücksichtigung der Sicherheitsfunktionen wirkt sich stark auf den Erfolg eines Projekts aus und motiviert zudem das Projektteam, die Security speziell für die Anforderungen jedes Unternehmensstandorts anzupassen.

5. Gründliche Tests vor der umfassenden Implementierung

Die Durchführung einer Machbarkeitsstudie in mehreren repräsentativen Standorten spart letztlich Zeit bei der Implementierung im gesamten Unternehmen. Ein SD-WAN nutzt eine Vielzahl von Bandbreiten-Optionen – MPLS, mobile Daten und Breitband-Internetzugänge –, um die Anforderungen verschiedener Benutzertypen mit unterschiedlichen Anwendungen zu erfüllen. Daher ist es praktisch unmöglich, das Verhalten eines derart komplexen Systems theoretisch vorherzusagen. Mit einem Proof of Concept können Sie die Endanwender-Erfahrung der verschiedenen Benutzerprofile bewerten sowie die technische und finanzielle Performance bei unterschiedlichen Betriebsbedingungen messen. Da daran auch die lokalen Teams beteiligt sind, wirkt sich das positiv auf die allgemeine Akzeptanz des SD-WAN-Projekts aus.

1 „Delivering large-scale IT projects on time, on budget, and on value.“ Mc Kinsey Okt. 2012

FORTINET

www.fortinet.com/de

Copyright © 2021 Fortinet, Inc. Alle Rechte vorbehalten. Fortinet®, FortiGate®, FortiCare® und FortiGuard® sowie bestimmte andere Marken sind eingetragene Marken von Fortinet, Inc. Bei anderen hier aufgeführten Namen von Fortinet kann es sich ebenfalls um eingetragene und/oder Gewohnheitsmarken von Fortinet handeln. Alle weiteren Produkt- und Unternehmensnamen sind u. U. Marken ihrer jeweiligen Eigentümer. Leistungs- und andere hierin enthaltene Kennzahlen stammen aus internen Labortests unter idealen Bedingungen. Die tatsächliche Leistung und andere Ergebnisse können davon abweichen. Keine der hierin enthaltenen Angaben stellt eine verbindliche Verpflichtung durch Fortinet dar und Fortinet lehnt alle ausdrücklichen oder implizierten Garantien ab. Ausnahme: Fortinet geht einen verbindlichen, schriftlichen Vertrag mit einem Käufer ein, der vom Leiter der Rechtsabteilung von Fortinet unterzeichnet wird und der eine ausdrückliche Garantie dafür gewährt, dass ein bestimmtes Produkt entsprechend den genau angegebenen Leistungskennzahlen bestimmungsgemäß funktioniert. In diesem Fall sind ausschließlich die in diesem verbindlichen, schriftlichen Vertrag aufgeführten spezifischen Leistungskennzahlen für Fortinet bindend. Jede diesbezügliche Garantie beschränkt sich einzig auf die Leistung unter den gleichen idealen Bedingungen wie bei den internen Labortests von Fortinet. Fortinet lehnt dementsprechend jegliche ausdrücklichen oder implizierten Verpflichtungen, Zusagen und Garantien ab. Fortinet behält sich das Recht vor, diese Veröffentlichung ohne Ankündigung zu ändern, zu bearbeiten, zu übertragen oder anderweitig zu überarbeiten. Es gilt die jeweils aktuellste Fassung der Veröffentlichung.

6. Schwerpunkt auf Transparenz

Sie können nicht kontrollieren, was Sie nicht sehen können. Da ein SD-WAN vor allem eine bessere Einbindung von Remote-Standorten bei gleichzeitiger Kostensenkung bringen soll, ist es wichtig, dass Sie mit Ihrer SD-WAN-Lösung auch überwachen können, ob und wie stark sich diese Vorteile bemerkbar machen. Selbst wenn Ihre Lösung einen Managed Security Service Provider (MSSP) umfasst, sollten Sie das Netzwerk mit einem Read-only-Dashboard im Auge behalten können. Dank dieser Transparenz können Sie sich auf strategischere Aufgaben konzentrieren und gleichzeitig die Metriken verfolgen, die sich auf Ihre Produktivität und die Einhaltung gesetzlicher Bestimmungen auswirken.

7. Objektive Bewertung durch neutrale Quellen

Die Kombination von Netzwerk- und Security-Funktionen in einer einzigen Lösung beinhaltet die Integration sehr vieler verschiedener Technologien. Jeder Anbieter wird natürlich die Bereiche betonen, in denen er am stärksten ist. Für eine unvoreingenommene Meinungsbildung zur SD-WAN-Implementierung in der Praxis sollten realistische Benutzererlebnisse und unabhängige Quellen einbezogen werden. Neutrale Einrichtungen wie die NSS Labs, die unabhängige externe Tests durchführen, können viel Hilfreiches beisteuern. Auch ein Blick in Gartners Magic Quadrants lohnt vor der Investition in ein SD-WAN.

Fazit

Nie zuvor war die Aufrechterhaltung einer allgegenwärtigen Konnektivität mit Remote-Standorten so wichtig. Ein SD-WAN kann dies nachweislich gewährleisten und eröffnet zudem Vorteile, die nur schwer von der Hand zu weisen sind, wie Kostensenkungen oder die Priorisierung von Anwendungen. Doch bei einem SD-WAN muss mehr berücksichtigt werden als nur der Netzwerk-Aspekt. Wie bei vielen Transformationslösungen kann die Vernachlässigung von Sicherheitsfragen zu ernsthaften Risiken, unzufriedenen Benutzern und Datenschutzverletzungen führen. Wenn Sie jedoch die hier genannten sieben Erfolgsfaktoren berücksichtigen, können Sie diese Nachteile nicht nur vermeiden, sondern auch die Rolle des CISO im digitalen Innovationsprozess stärken.