BASYS BRINOVA
part of connexta

Sicherheit im Homeoffice

Der Heimarbeitsplatz als Risiko für das Unternehmensnetzwerk

Ob im Rahmen des Modern Workplace oder eines Business Continuity Plans, das Thema Homeoffice boomt. Steht bei Ihnen nur die Produktivität der Mitarbeitenden im Vordergrund?

Besonders wenn eine Krisensituation die schnelle Umsetzung einer Homeoffice-Lösung im Rahmen der Business Continuity erfordert ist es wichtig, nicht überstürzt zu handeln. Neben dem zuverlässigen und praktischen Remote-Zugriff auf Unternehmensressourcen und der Mitarbeiterproduktivität sollte vordergründig auch immer die Kontrolle über den Zugriff und die Sicherheit dieser Lösung betrachtet werden. Kurzfristig umgesetzte Änderungen, die die IT- und Informationssicherheit des Unternehmens betreffen, bieten häufig Angriffsvektoren für das Unternehmensnetzwerk. Wir beraten Sie gerne dabei, mit Bedacht eine langfristige Strategie zu entwickeln und Ihr IT-Sicherheitskonzept ideal zu ergänzen, um die Gefahr von Datenmanipulation und Cyberangriffen auch im Homeoffice zu minimieren. Neben technischen Lösungen gehört dazu ebenso die stetige Information und Sensibilisierung der Mitarbeiter sowie die Entwicklung verbindlicher Richtlinien.

Der Baustein für Ihr IT-Sicherheitskonzept

Zur Umsetzung eines abgesicherten Zugangs zu Ihrem Firmennetzwerk bieten wir Ihnen stets eine individuelle und kompetente sowie herstellerunabhängige Beratung, Lösungskonzeption und Implementierung.

Für eine ausreichende Sicherheit im Homeoffice empfehlen wir Ihnen als Baustein für Ihr IT-Sicherheitskonzept unter anderem:

- Conditional Access
- MFA
- SSL-VPN
- VDI

Schutz der Zugangsdaten und des Clients

- Multi-Faktor-Authentifizierung (MFA) schützt den Zugang durch den Aufbau einer zusätzlichen Hürde.
- Ergänzende Authentifizierungsmethoden via Token, App oder Biometrie sind sicherer als jedes starke Passwort.

Überprüfung der Zugangsberechtigung durch mehrere unabhängige Faktoren.

Schutz des Firmennetzwerkes und der Firmendaten

- Der Einsatz eines "Medienbruchs" kapselt den Client ab und schafft eine sichere Daten-schleuse zum Firmennetzwerk.
- Grundsätzliches Misstrauen allen Diensten, Anwendern und Geräten gegenüber (Zero-Trust-Prinzip) schließt sowohl externe als auch interne Gefahrenpotenziale aus.

Erhöhte Kontrolle durch einen abgesicherten Datentransfer.

Produktivität und Benutzerfreundlichkeit

- Verringerung des Administrationsaufwands durch eine schnelle und unkomplizierte Zuordnung von Geräten und Benutzern.
- Konsistenter Benutzerkomfort auf allen Geräten – egal ob Firmengerät oder BYOD.

Zentrales, zeit- und kostensparendes Regelwerk für dynamische Bürokonzepte.

> Trotz notwendiger kurzfristiger Realisierung unserer Homeoffice-Arbeitsplätze ist es gelungen, schnell eine produktive Arbeitsumgebung für alle Mitarbeiter zu schaffen – ohne Kompromisse in puncto Sicherheit einzugehen. Dank der intensiven Beratung sind wir umfassend geschützt und fühlen uns gut gerüstet für die Zukunft.
> IT-Leiter eines nordwestdeutschen Handelsunternehmens

Sicherheit im Homeoffice

Zusammenfassung der Lösung

Conditional Access

- Regelbasierte Authentifizierung schützt unternehmenskritische Daten und Bereiche vor unbefugtem Zugriff, da nur berechtigte Nutzer, Endgeräte und Anwendungen verwendet werden können.

Multi-Faktor-Authentifizierung

- Selbst wenn ein Angreifer die Benutzername-Passwort-Kombination kennt, kann kein Zugriff auf den Account erfolgen.
- Das zusätzliche Authentifizierungsverfahren ist nur dem Anwender bekannt und kann nicht ohne Weiteres nachvollzogen bzw. dupliziert werden.

SSL-VPN

- Ermöglicht eine gesicherte Verbindung und einen Zugang auf bestimmte Dienste, ohne einen direkten Zugriff auf das gesamte Unternehmensnetz freizugeben.
- Kontrolle über das, was innerhalb des VPN-Tunnels geschieht.

Virtual Desktop Infrastructure

- Zentralisierung der gesamten Administration (Patches, Aktualisierungen, Konfigurationen und Durchsetzung von Richtlinien) auf einem Server im Rechenzentrum für eine einheitlich sichere Umgebung.
- Bei Diebstahl des Endgeräts können keine vertraulichen Daten vom lokalen Speicher abgerufen werden, da die Daten auf dem Server und nicht auf dem Gerät gespeichert sind.

Unser Versprechen an Sie

Wir bieten Ihnen die optimale Unterstützung, gezielt auf die ständig wachsenden Sicherheits-anforderungen der internetbasierten Arbeitswelt reagieren zu können.

Unsere IT-Consultants und System-spezialisten entwickeln gemeinsam mit Ihnen das für Sie optimal passende Service-Angebot.

Ein Angebot zum Einstieg

- Die Preisgestaltung ist flexibel und richtet sich nach Ihrer individuellen Umgebung und den von Ihnen gebuchten Leistungspaketen.

Konkrete Vorteile / gewünschte Ergebnisse

- Sichere Arbeitsumgebung mit umfassendem Schutz vor internen und externen Bedrohungen
- Die Mitarbeiterzufriedenheit erhöht sich durch einen einheitlichen Benutzerkomfort auf allen Geräten
- Vertrauensvolle Zusammenarbeit, persönliche Betreuung und regionale Nähe

Warum BASYS Brinova?

BASYS Brinova liebt und dient dem Mittelstand seit über 30 Jahren. Unsere IT-Berater analysieren Ihre Bedürf-nisse und besprechen im Anschluss mit Ihnen die richtigen Schritte. Mit uns bekommen Sie die sichere Arbeits-umgebung, die perfekt zu Ihrem Unternehmen passt. Dies haben wir bereits in zahlreichen Branchen unter Beweis gestellt, auch in sensiblen Bereichen wie etwa Banken & Versicherungen sowie dem Gesundheitswesen.

A BASYS Brinova GmbH | Hermine-Seelhoff-Straße 1-2 | 28357 Bremen E info@basys-brinova.de W www.basys-brinova.de