Warum Firmen jetzt die Chance auf mehr Flexibilität, Produktivität und IT-Sicherheit haben

Nach rund 1,5 Jahren Pandemie dachten viele, das Arbeitsmodell „Homeoffice" würde auch in Deutschland zum neuen Standard werden. Nun geht es vielerorts zurück in die Büros, während andere die Büroflächen reduzieren und komplett auf Homeoffice setzen. Doch warum eigentlich für eine Seite entscheiden, wenn man sich flexibel aufstellen und die Vorteile beider Arbeitswelten nutzen kann?

Von Dennis Christ, NCP engineering GmbH

Wer vor dem Frühjahr 2020 einem klassischen „Büro-Job" nachging, der tat das laut Bitkom mit 82-prozentiger Wahrscheinlichkeit genau dort: im Büro. Ein Kunden-Meeting am Küchentisch? Für die meisten, wenn überhaupt, nur in Ausnahmen denkbar. Warum sollten Mitarbeiter im potenziell unsicheren Heimnetzwerk tätig sein, wenn sie innerhalb der IT-Sicherheit des Unternehmens direkt auf den Firmenserver zugreifen können? Ob dieser Schutz auch im Heimnetzwerk der Mitarbeiter gegeben ist? Sicherlich in vielen Fällen nicht, wie eine Studie der ESET Deutschland GmbH zeigt – und so waren alle Homeoffice-Überlegungen an diesem Punkt oft schon zu Ende gedacht oder brachten unangenehme Kompromisse mit sich.

> *„Jeder zweite Homeoffice-Arbeitsplatz in Deutschland ist unsicher."*
>
> *„Quo Vadis, Unternehmen?" - ESET Deutschland GmbH*

Keine Zeit für den Ausbau der Homeoffice-Strukturen

Was die Pandemie in den letzten 18 Monaten für IT-Abteilungen weltweit bedeutete, muss an dieser Stelle nicht weiter ausgeführt werden. Selbst wenn die Herausforderungen vielfältig waren, verband praktisch alle Unternehmen eine Gemeinsamkeit: Wer seinen Aufgaben von zu Hause nachgehen konnte, wurde ins Homeoffice geschickt – so wollte es schließlich die „Corona-Arbeitsschutzverordnung" der Bundesregierung.

Um dies in der Kürze der Zeit zu realisieren, haben sich Unternehmen vor allem zu Beginn der Krise eine einfach beschaffbare Remote-Access-Lösung zugelegt. Laut Statista stieg so der Anteil an Homeoffice-Arbeitern bis zum April 2020 von 4 Prozent auf 27 Prozent schlagartig an. Rundum sichere Anbindung der Heimarbeitsplätze? Flexibilität des Lizenzbestands? Einfache Administration der Umgebung? Für die Klärung solcher Punkte blieb da jedoch meist keine Zeit. Hauptsache es ging schnell, und die Mitarbeiter konnten halbwegs vernünftig von zu Hause aus arbeiten.

Genau hier lag jedoch das Problem: Halbwegs vernünftiges Heimarbeiten klappte in vielen Fällen nicht. Denn es gab zu diesem Zeitpunkt weit mehr Unternehmen ohne organisatorische und technische Homeoffice-Möglichkeiten als man denken würde. Die anfangs schnell aufgesetzten Fernzugriffslösungen führten zu technischen Problemen, weshalb sich die Mitarbeiter nicht stabil mit den Firmenservern verbinden konnten. Dies verursachte wiederum einen erheblichen Mehraufwand für IT-Verantwortliche, von denen laut einer Pure-Storage-Umfrage 72 Prozent die Arbeit in der Pandemie als echten Stresstest empfanden.

Schlimmstenfalls stellten die schnell eingeführten Technologien sogar ein Sicherheitsrisiko für das Firmennetzwerk dar. Diesen Punkt machten sich auch Cyber-Kriminelle zunutze. So ist es wenig verwunderlich, dass die Gesamtzahl an neuer Malware laut der IT-Sicherheitsplattform SoSafe im Jahr 2020 einen neuen Höchstwert von 750 Millionen erreichte.

Cyber-Angriffe haben Hochkonjunktur

Genau hier rückt ein wichtiger Aspekt in den Mittelpunkt jeder „Post-Corona-Planung": Die IT-Welt dreht sich bekanntlich besonders schnell weiter – leider auch im negativen Sinn. Cyber-Kriminelle waren im vergangenen Jahr so aktiv wie nie, und dieser Trend wird sich nicht wieder umkehren. So wurden im ersten Halbjahr 2021 weltweit 304,7 Millionen Ransomware-Angriffe registriert – was bereits die

Gesamtzahl für das komplette Jahr 2020 übertrifft (304,6 Millionen).

Wie die weltweit angelegte Studie „The State of Ransomware 2021“ von Sophos zeigt, werden dabei insbesondere die finanziellen Auswirkungen solcher Angriffe für Unternehmen immer gravierender. Durchschnittlich 1,5 Millionen Euro mussten Firmen aufbringen, bis sie sich vollständig von einer Ransomware-Attacke erholt hatten. Dazu gehörten auch Kosten durch Produktionsstillstand, verlorene Aufträge oder Wissensverlust – denn gerade einmal erschreckende acht Prozent aller betroffenen Unternehmen erhielten ihre Daten vollständig zurück.

Die IT-Sicherheitsgefahren für Unternehmen werden also zukünftig nur noch gravierender – und vor diesem traurigen Trend kann sich ein Unternehmen nicht schützen, indem es wieder auf seinen IT-Infrastruktur-Stand von 2019 zurückkehrt.

Flexibel auf nicht planbare Situationen reagieren

Unternehmen müssen sich daher die Frage stellen, wie sich der Schutz vor zunehmender Cyber-Kriminalität und die Entlastung der internen IT-Abteilung sicherstellen lassen, während man gleichzeitig flexibel auf künftige, nicht vorhersehbare Ereignisse reagieren kann. Für letztere ist keine weltweite Pandemie nötig. Spontane Hindernisse auf dem Arbeitsweg kennt jeder von uns – sei es ein platter Fahrradreifen am Morgen, ein verspäteter Zug oder ein scheinbar undurchdringbarer Verkehrsstau.

Mit solchen Problemen mussten die mehr als 10 Millionen Deutschen nicht kämpfen, die laut Bitkom während der Corona-Pandemie ausschließlich im Homeoffice gearbeitet haben – für 68 Prozent aller Arbeitnehmer stellt der Zeitgewinn durch Remote Work laut DAK-Studie sogar einen großen Pluspunkt dar.

Arbeitnehmer schätzen im Homeoffice am meisten

Quelle: Sonderanalyse zum DAK-Gesundheitsreport

Produktiv und sicher

Im Sinne der „Business Continuity“ erweist es sich als sinnvoll, wenn notfalls von zu Hause genauso produktiv und sicher gearbeitet werden kann wie im Büro. Damit das funktioniert, braucht es eine durchdachte, flexible und sichere Remote-Access-Anbindung, die nicht nur eine unkomplizierte Fernarbeit für Angestellte ermöglicht, sondern dabei auch Eindringlinge aus dem Firmennetz fernhält – während gleichzeitig der Administrationsaufwand für die interne IT geringgehalten wird.

Dafür empfiehlt sich eine ganzheitliche, softwarebasierte VPN-Lösung, wie sie unter anderem NCP als deutscher Hersteller aus Nürnberg anbietet. Eine solche Remote-Access-Softwarelösung sichert den kompletten Datenaustausch zwischen dem Anwender und dem Firmennetzwerk ab und lässt sich dank Hochskalierbarkeit in kürzester Zeit für hunderte oder tausende Anwender ausrollen.

Einfach zu administrieren und budgetschonend

Ein großer Vorteil einer solchen Lösung besteht in der einfachen Administrierbarkeit: IT-Verantwortliche können mittels einer zentralen Management-Umgebung Nutzer in Gruppen unterteilen und Policy-Änderungen automatisch für alle Anwender ausrollen. Die langwierige Konfiguration einzelner Clients entfällt damit komplett, wodurch sich auch große Umgebungen ohne viel Aufwand verwalten lassen. Dank weitreichender Software-Kompatibilität kann eine entsprechend ausgelegte Remote-Access-Lösung auch einfach in bestehende IT-Infrastrukturen integriert werden.

Hält das VPN-Produkt dann noch Nutzer-Clients für alle Endgeräte-Typen und Betriebssysteme bereit und ist komplett softwarebasiert, macht sich die IT-Abteilung damit unabhängig von Hardware-Lieferengpässen, die laut Foxconn noch bis in den Sommer 2022 anhalten können. Da Neuanschaffungen überflüssig werden, schont man auf diese Weise auch das IT-Budget. Dadurch können unter Umständen längst notwendige Investitionen im Bereich Cyber-Security getätigt werden, für den über 50 Prozent der Firmen laut Bundesamt für Sicherheit in der Informationstechnik (BSI) nicht einmal ein Zehntel ihrer IT-Ausgaben reservieren.

Im Punkt Budgetierung kann sich das Unternehmen zudem mit bedarfsgerechten VPN-Lizenzmodellen wie beispielsweise „Pay per Use“ oder sogar „Temporary Use“ besonders flexibel aufstellen. Durch ein solches Paket verfügt die Firma immer über einen einfach erweiterbaren Grundstock an VPN-Zugängen, während sie gleichzeitig zum Beispiel in der Urlaubszeit nicht für ungenutzte Zugänge aufkommen muss.

Die Notwendigkeit moderner VPN-Lösungen haben viele Unternehmen bereits erkannt. So sagen 75 Prozent der Firmen, dass VPN wichtig sei, um auch künftig auf unvorhergesehene Ereignisse und Pandemien effizienter reagieren zu können. Der Aufbau einer sicheren und dynamischen VPN-Infrastruktur ist somit auch langfristig von hoher Relevanz.