Home Office

Sichere Kommunikation ist unser Kerngeschäft

Unternehmen haben für die sichere Anbindung ihrer mobilen Mitarbeiter und der Kollegen im Home Office an das Unternehmensnetzwerk zu sorgen. Gerade das Home Office muss nun als ein wichtiger Faktor für »Business Continuity« gesehen werden.

Wir sprachen mit Patrick Oliver Graf, CEO & Managing Director bei NCP engineering, über die Veränderungen, die die Corona-Krise für den Arbeitsplatz der Mitarbeiter mit sich gebracht hat.

? Wie kann sichere Kommunikation gewährleistet werden?

Hier sind mehrere Faktoren entscheidend: Sichere Kommunikation fängt beim Mitarbeiter an, wie gut ist er geschult und auch für das Thema »Sicherheit« sensibilisiert, welche Lösungen verwendet er für seine tägliche Arbeit und natürlich ist auch das Thema »Vertrauen« in den Mitarbeiter ganz entscheidend. Technisch betrachtet, setzt es die Verwendung von entsprechend sicheren Kommunikationslösungen wie VPN voraus, beispielsweise bei der Anbindung von mobilen Geräten mit entsprechend sicheren Anmeldemechanismen. Aber auch die »Gesundheit« des eingesetzten Endgeräts ist hier entscheidend (Anti-Schadsoftware-Produkte, alles auf dem aktuellen Stand).

? Was trägt sichere Kommunikation zu Unternehmenszielen bei?

Sichere Kommunikation ist in diesen digitalisierten Zeiten ein entscheidender Faktor zur Erreichung beziehungsweise Sicherung der Unternehmensziele. In den vergangenen Monaten wurden immer wieder Fälle bekannt, in denen Unternehmen schwerste Schäden durch Ransomware oder durch andere Schadsoftware zugefügt wurde und deren Auswirkungen noch Monate danach zu spüren sind.

? Das Home Office ist in den letzten Wochen erwachsen geworden. Wie sehen Sie die momentane Situation für Firmen und deren Mitarbeiter?

Home Office wurde bisher als eine Art Mitarbeiter-Benefit gesehen, ein stückweit sollte es eine positive Ergänzung zur »Work-Life-Balance« sein. Bereits das Sturmtief »Sabine« hat gezeigt, dass das dezentrale Arbeiten ein wichtiger Faktor sein kann. Seit Ausbruch des Corona-Virus müsste nun jedem klar sein, welchen Stellenwert das Home Office für Unternehmen und auch deren Mitarbeiter hat. Unternehmen, die sich bisher zurückhaltend mit dem Thema beschäftigt haben, sehen sich heute mehr oder minder gezwungen schnell zu handeln. Hierzu müssen auf der einen Seite die technischen Voraussetzungen geschaffen werden, was spontan nicht ganz so einfach sein kann, auf der anderen Seite muss aber auch dem rechtlichen Rahmen Rechnung getragen werden. Ich erinnere hier nur an die Einhaltung der DSGVO und Aspekte des Arbeitsschutzes. Eines ist aber auch klar: nicht jeder Arbeitsplatz ist gleichzeitig auch als Home-Office-Arbeitsplatz geeignet. Das kann durchaus zu »Schwingungen« innerhalb der Belegschaft führen, da sich einige Mitarbeiter benachteiligt fühlen könnten, in dem man sie nicht im Home Office arbeiten lässt.

? Wie hat die Corona-Pandemie das Thema Home Office weltweit verändert?

Ich denke eine weltweite Bewertung ist sehr schwierig. In vielen Ländern war Home Office (Work from Home) mehr oder weniger schon existent, etwa in den USA und wie gesagt, auch hier. Dass wir das Home Office in Zukunft als festen Bestandteil eines Unternehmensnetzwerk mit einbeziehen müssen liegt jetzt auf der Hand. Home Office muss nun als ein ganz wichtiger Faktor für »Business Continuity« gesehen werden.

? Alle sprechen von Digitalisierung. Einige sind weit, andere am Anfang. Welche Schwierigkeiten sehen Sie bei / neben der »Digitalisierung« des Home-Arbeitsplatzes?

Neben den technischen Herausforderungen gibt es auch andere Punkte/Schwierigkeiten, die beachtet werden müssen. Unternehmensprozesse müssen sich verändern beziehungsweise anpassen, alleine schon, weil deutlich weniger persönliche soziale Kontakte stattfinden. Ein schneller Austausch, eine schnelle Abstimmung wie man es im Büro gewohnt war, wird schwieriger. Konferenzsysteme erhalten einen höheren Stellenwert. Zudem wir die »Kontrolle der Produktivität« ebenso erschwert. Ein Home Office birgt auch ein höheres Ablenkungspotenzial in sich, die Art und Weise der Mitarbeiterführung verändert sich.

? Mit welchen Problemen sind die Unternehmen konfrontiert und wie lösen sie diese? Wie gut sind die Unternehmen aus Ihrer Sicht aufgestellt?

Unser Kerngeschäft ist es Unternehmen die sichere Anbindung ihrer mobilen Mitarbeiter und Mitarbeiter im Home Office an das Unternehmensnetzwerk zu ermöglichen. Daher wissen wir, dass sich viele Unternehmen dahingehend aufgestellt hatten. Die große Herausforderung, die Unternehmen im Rahmen der Pandemie jetzt auf einmal bewältigen mussten war, in kürzester Zeit für massiv viele Anwender einen Home-Office-Betrieb zu ermöglichen. Das ist mit unserer Lösung ohne weiteres möglich gewesen. Einige Unternehmen mussten leider feststellen, dass viele Produkte nicht skalieren und sich auch nur schwer erweitern lassen beziehungsweise teilweise ungeeignet sind.

Was machen Firmen, die das Thema Home Office bisher als unwichtig abgetan haben?
Für die war, wie gesagt, bereits das Sturmtief »Sabine« eine erste Warnung. Seit Ausbruch der Corona-Viruspandemie sollten auch diese davon überzeugt sein, dass man IT-technisch zukünftig auf ein Home Office als festen Bestandteil nicht verzichten kann um einen unterbrechungsfreien Betrieb zu gewährleisten, unabhängig ob aus Gründen einer Pandemie oder wettertechnischen Kapriolen.

Vor wenigen Wochen galten Ransomware und Trojaner als größtes Risiko für die Arbeitswelt. Jetzt zwingt die Corona-Krise weltweit Unternehmen, ihre Mitarbeiter über Home Office arbeitsfähig zu halten. Darunter sind auch Unternehmen, die bisher keine dezidierte Lösung für den Heimarbeitsplatz vorgehalten haben. Die Gefahr: Im Hauruck-Verfahren können völlig neue Risiken auftreten, darunter auch IT-Bedrohungen, die im Büro am Küchentisch nicht mehr an einer Firmen-Firewall scheitern können. Was meinen Sie hierzu?
Unternehmen investieren jährlich Millionenbeträge in IT-Sicherheit für ihr Netzwerk. Das private Netzwerk, in dem auf einmal ein Home Office entsteht, ist vergleichsweise schwach bis gar nicht abgesichert. Wer in zukünftigen Architekturen das Thema Home Office stiefmütterlich behandelt und nicht mit in die Sicherheitsarchitektur des Unternehmens einbezieht, wird sich eher über kurz als lang der gleichen Situation ausgeliefert und möglicherweise einem bösartigen Angriff ausgesetzt sehen.

Mitarbeiter ohne Dienst-Notebook müssen im Corona-Ausstand auf private Geräte zurückgreifen. Dies stellt eine enorme Gefahr dar. In privaten Systemen verbergen sich nicht selten Schädlinge, die nicht kontrolliert werden können und per VPN sogar ungeschützten Zugang zu einem Firmennetzwerk bekommen. Wie sehen Sie das?
Die Einbeziehung von privaten Endgeräten kann in der Tat ein großes Sicherheitsrisiko darstellen. Hier müssen auf dem PC erst entsprechende Voraussetzungen geschaffen werden. Abgesehen vom sicheren Zugang und einer sicheren Anmeldung (etwa Zweifaktor-Authentifizierung) über VPN, der sich beispielsweise bei der NCP-Lösung rechte- und sicherheitstechnisch konfigurieren lässt.

Die IT-Sicherheit eines Heimarbeitsplatzes ist ebenso wichtig wie die Sicherheit des Firmennetzwerks. Wie können qualitative Standards (etwa Geschwindigkeit, die für einen externen Zugriff auf das Unternehmensnetzwerk nötig sind) gewährleitet werden?
Das Thema verfügbare Geschwindigkeit beziehungsweise Bandbreite im Home Office kann durchaus problematisch sein. Alternativ stehen aber in der Regel auch mobile Netze (3G/4G/LTE) zur Verfügung, über die eine Anbindung über das eigene Smartphone als Hotspot, ermöglicht wird. Die klassischen »Road Warriors« oder auch »digitale Nomaden« genannt, die den »Modern Workplace« leben und die so gut wie jeden Ort als Arbeitsplatz verwenden sind natürlich speziell abzusichern. Hier greifen Technologien von NCP für eine sichere Anmeldung am öffentlichen Hotspot und der Definition der Unterscheidung von »freundlichen« und potenziell »feindlichen« Netzwerken, wobei ein freundliches Netzwerk das Heimnetz des Mitarbeiters ist und ein öffentlicher Hotspot als feindlich eingestuft werden kann, mit entsprechender Einschränkung der Funktionalität bis hin zum Verwehren der Verbindung.