Sicheres Home Office für Mitarbeiter einrichten

IT-Sicherheit und Telefonie über VPN & Co.

In dieser ersten Podcast-Folge von BREKOM spricht Vertriebs-Mitarbeiter Michael Schneider über die Herausforderungen und Risiken des (un)sicheren Home Office, denen sich viele Unternehmen vor allem in der Corona-Krise kurzfristig stellen mussten. Antworten auf seine Fragen rund um die Einrichtung eines sicheren Home Office geben ihm dabei TK-Experte Heiko Bulmahn und IT-Security-Spezialist Sebastian Pfeiffer aus dem Consulting bei BREKOM.

INHALT

1 Nutzung privater Telefone im Home Office – ja oder nein? 1

2 Welche Alternativen zur Telefonie im Home Office gibt es? 2

3 Wie kann ich die Verbindung aus dem Home Office zur Firmen-Telefonanlage herstellen und was brauche ich dafür? 3

4 IT-Security und VPN – Was ist das und was sind die Voraussetzungen dafür? 4

5 Wie kann ich als Arbeitgeber die Performance sicherstellen? 5

6 Wie kann ich den Mitarbeiter optimal mit dem Firmennetzwerk und der Telefonanlage verbinden und so seine Erreichbarkeit sicherstellen? 5

7 Warum sollte der Mitarbeiter nur über die Firmen-Rufnummer kommunizieren? 6

8 Wie kann ich als Administrator die Sicherheit und Performance der Unternehmens-IT-Infrastruktur überprüfen? 7

9 Welche Risiken birgt eine schlechte Netzwerkverbindung für die Telefonie über VPN und wie kann ich diese vermeiden? 8

10 Wie kann ich verschlüsselte Verbindungen für Datenverkehr und Telefonie sicherstellen – und muss ich das überhaupt? 8

1 Nutzung privater Telefone im Home Office – ja oder nein?

Michael Schneider: In der Corona-Zeit haben uns viele Anfragen unserer Kunden erreicht, die zu dem Zeitpunkt nicht wussten: Wie gehe ich mit meinen Mitarbeitern im Home Office um? Wie schaffe ich ein sicheres Home Office und ein Umfeld, in dem der Mitarbeiter sich nicht nur sicher, sondern auch gut mit dem Unternehmensnetzwerk verbinden kann? Und was sind dort die Vor- und Nachteile in den Bereichen Telekommunikation und IT-Security? Auf diese und weitere Fragen versuchen wir heute Antworten zu finden.

Widmen wir uns doch zuerst dem Telefonie-Bereich. Nehmen wir an, ein Unternehmen möchte, dass seine Mitarbeiter mit ihrem privaten Festnetz- oder Mobiltelefon arbeiten im Home Office. Was wären da die Vor- und auch die Nachteile?

Heiko Bulmahn: Ganz klassisch wird meistens zuerst das Gespräch von der Firma einfach dauerhaft umgeleitet, also eine ganz normale Anrufumleitung eingerichtet. Dann ist man zwar erreichbar zuhause unter seiner Firmennummer für den ersten Call, es gehen aber sämtliche Firmen-Leistungsmerkmale verloren. So würde beispielsweise eine Chef-Sekretär-Funktion nicht mehr funktionieren oder der Anruf würde nicht mehr sauber durchgesteuert werden, was besonders im Call-Center-Bereich relevant ist. Und sobald ich unter diesen Voraussetzungen abgehend telefoniere, erscheine ich in dem Fall beim Kunden mit meiner Privatnummer – das ist natürlich alles andere als professionell.

2 Welche Alternativen zur Telefonie im Home Office gibt es?

Heiko Bulmahn: Deshalb gibt es diverse andere Lösungen, die dafür sorgen, dass die Firmen-Rufnummer derart durchgestellt wird ins Home Office, dass man auch von zuhause aus unter seiner Firmennummer sichtbar wird beim Kunden.

Dafür kann man wie eine Art Remote Access Worker eingerichtet werden, wofür bei den unterschiedlichen TK-Herstellern unterschiedliche Mechanismen notwendig sind, oft müssen dazu auch Lizenzthemen geklärt werden. Man kann dann entweder mit einem normalen Telefon arbeiten, oder aber mit einer App auf dem Handy dafür, das ist auch wiederum vom jeweiligen Hersteller und dessen Leistungsmerkmalen abhängig.

Man kann es auch so machen, dass die Telefonanlage von der Firma einen zuhause anruft, man geht ran und dann wird der eigentliche Call über die Firmenanlage aufgebaut, sodass der Anrufer gar nicht merkt, dass ich als Mitarbeiter in Wirklichkeit zuhause sitze – bis vielleicht die Kinder im Hintergrund schreien oder der Hund bellt. Das Ganze kann man auch als Steigerung mit einem Softphone machen, dann muss man kein Hardware-Endgerät mehr von zuhause benutzen oder eines von der Firma mit nach Hause nehmen.

In dem Fall, dass ich über ein solches Softphone ins Firmennetzwerk rein möchte, muss aber die Anlage dafür geeignet sein, es müssen also entsprechende Hardwarevoraussetzungen und Lizenzen gegeben sein. Worüber ich mir dann auch Gedanken machen muss, ist, dass solche Sachen oftmals nicht über Citrix möglich sind, es gibt zwar hier und da Lösungen dafür, aber um den vollen Funktionsumfang der Firmenanlage nutzen zu können, brauche ich in vielen Fällen einen VPN-Zugang.

Michael Schneider: Also würdest du sagen, privates Festnetz- oder Mobiltelefon sollte man grundsätzlich nicht in Betracht ziehen?

Ich selbst sehe da auch insofern noch den Nachteil für den Mitarbeiter, wenn dieser den Kunden mit seiner Privatnummer anruft, hat der Kunde natürlich dann auch die Möglichkeit, jederzeit beim Mitarbeiter privat anzurufen. Das kann dann auch mal abends sein, wenn Frau oder Kind ans Telefon gehen und der Kunde sich wundert, wen er da am anderen Ende der Leitung hat.

Also würdest du schon grundsätzlich sagen, möglichst das geschäftliche Mobiltelefon nutzen oder aber eine Verbindungsmöglichkeit versuchen herzustellen, dass man mit der Geschäftsnummer auch von zuhause aus telefonieren könnte?

Heiko Bulmahn: Ja, gerade letzeres ist für viele wichtig. Man muss sicherlich auch differenzieren, in was für Bereichen ich da unterwegs bin: Wenn ich, sagen wir mal, als normaler Sachbearbeiter nur ein bis zwei Telefonate am Tag im Rahmen eines Projekts tätige, dann kann man das eventuell tolerieren, dass man auch mal mit einer Nicht-Firmen-Telefonnummer agiert – vorausgesetzt, man selber kann und will das verantworten und der Arbeitgeber hat kein Problem damit. Aber wenn ich jetzt beispielsweise im Bereich Vertrieb bin, wo ich als Firma auch etwas verkaufen möchte oder eine Dienstleistung erbringe, ist immer dazu zu raten, dass man die Telefonie so professionell einrichtet, dass der potenzielle Kunde davon nichts merkt.

Das hat auch den Vorteil, dass wenn man das ein Mal vernünftig einrichtet, der Mitarbeiter langfristig flexibel ist mit seinem Arbeitsplatz. Auch wenn die Corona-Zeiten irgendwann mal vorbei sind, bleiben die Mitarbeiter weiterhin mobil mit ihrem Arbeitsplatz für Dienstreisen und Co., ohne dass der Anrufer etwas davon mitbekommt, wo der Mitarbeiter sitzt.

3 Wie kann ich die Verbindung aus dem Home Office zur Firmen-Telefonanlage herstellen und was brauche ich dafür?

Michael Schneider: Wie muss ich mir das dann genau vorstellen? Habe ich dann die Möglichkeit, als Mitarbeiter zuhause ein physisches Telefon, ähnlich wie ich es jetzt im Büro habe, zu betreiben? Kann ich das dann so anstöpseln an meine Fritzbox? Oder gibt's die Möglichkeit, eine App oder ein Programm auf meinem Notebook zu nutzen und dann ein sogenanntes Softphone zu betreiben? Oder welche Alternativen gibt es da noch?

Heiko Bulmahn: Es gibt da eine ganze Palette an Lösungsmöglichkeiten.

Fangen wir mit der einfachsten Lösung an: Wenn ich ein Softphone auf dem Notebook installiere, dann brauche ich eigentlich nur einen gesicherten Zugang ins Unternehmensnetzwerk, mehr nicht. In den meisten Fällen brauche ich dafür wie gesagt einen VPN-Zugang, weil das Softphone sich dann mit dem Callserver von der zentralen Telefonanlage verbinden möchte. Seltener klappt es auch mal mit Citrix-Zugängen, aber das hängt immer vom Leistungsumfang der Hersteller ab.

Eine weitere Variante wäre das Festnetztelefon oder IP-Endgerät von der Firmen-Telefonanlage, das der Mitarbeiter mit nach Hause nimmt und dort dann an die Fritzbox anschließt. Hierfür sollten aber nur Geräte mit einem VPN-Client genutzt werden, da werden entsprechend auch Zertifikate reingeladen, damit die Geräte sich quasi über das Internet vom Heimanwender mit der gesicherten Firmenumgebung verbinden. In dem Fall ist es so, als würde ich das Telefon ganz normal im Büro benutzen, mit meiner Rufnummer aus dem Firmennetz.

Wiederum eine andere Variante wäre es, das private Telefon des Mitarbeiters zu nutzen, auf das dann entweder eine App kommt oder das so intelligent in der Anlage eingerichtet wird mit den entsprechenden Lizenzen, dass eine Art Dreierkonferenz zwischen dem Mitarbeiter, der Firmen-Telefonanlage und dem Anrufempfänger hergestellt wird. Das geht in Bruchteilen von Sekunden, sodass der Anrufempfänger davon nichts mitkriegt. Ich übermittle meinen Anrufwunsch nicht direkt zum Endkunden, sondern teile eigentlich der Telefonanlage mit, wen ich erreichen möchte, diese wählt dann für mich und innerhalb von Bruchteilen einer Sekunde wird das Ganze wie eine Dreierkonferenz zusammengeschaltet. So tauche ich bei dem Anrufempfänger mit meiner bekannten Firmen-Rufnummer auf.

Je nach Anwendungszweck und Anforderungen meiner täglichen Arbeit reicht vielleicht die letzte Variante aus, aber wenn ich den vollen Funktionsumfang der Telefonanlage benötige, weil ich beispielsweise im Call Center oder mit einer Chef-Sekretär-Anlage arbeite, komme ich mit den einfachen Varianten nicht mehr aus. In solchen Fällen muss man wirklich projektspezifisch gucken, welche Variante in welchem Umfang die sinnvollste für die jeweiligen Anforderungen ist.

Das hängt oftmals auch damit zusammen, welche Softwarestände und welchen Herstellertyp von TK-Anlage ich im Unternehmen vorliegen habe. Grundsätzlich kann man sagen, geht eigentlich mit allen Herstellern im weitesten Sinne alles, allerdings ist es oftmals in der Vergangenheit so gewesen, dass dann nicht mehr die aktuellen Softwarestände in der Anlage vorhanden waren, wodurch man dann wiederum Security-Themen vor sich hat. Das ploppt dann alles auf und das ist in Zeiten der Corona-Krise natürlich vielen auf die Füße gefallen, die vorher gesagt haben „brauchen wir alles nicht“.

Wir haben‘s im eigenen Unternehmen ja auch gemerkt, als das Ganze dann Fahrt aufgenommen hatte, konnte es einigen Kunden gar nicht schnell genug gehen. Also es gab Kunden, die noch im Februar gesagt haben „brauchen wir nie“ und im März sagten die „Wann könnt ihr liefern, könnt ihr das nicht morgen schon für 100 Leute installieren?“. Also solche Fälle hatten wir auch.

4 IT-Security und VPN – Was ist das und was sind die Voraussetzungen dafür?

Michael Schneider: Du hast zwei gute Stichworte geliefert: VPN und Security. Da würde ich dann gerne Sebastian mit ins Boot holen, weil das dann natürlich ebenfalls immens wichtige Punkte sind: Ich verbinde mich dann mit meinem Telefon ins Firmennetz und nehme Verbindung zur TK-Anlage auf, auch das sollte ja möglichst in gesicherter Form stattfinden. Sebastian, was würdest du da als Kriterien sehen, um eine sichere VPN-Verbindung herzustellen, oder vielleicht magst du überhaupt erstmal erklären, was ist überhaupt VPN und wie kann ich sicherstellen als Administrator aus dem Security-Bereich, ob mein Netzwerk wirklich über diese Merkmale verfügt?

Sebastian Pfeiffer: Genau, also fangen wir erstmal an bei VPN: VPN beschreibt eigentlich eine ganze Palette an Lösungen, die dafür gedacht sind, eine sichere Verbindung über ein unsicheres Medium zu schaffen. Im Normalfall heutzutage ist das unsichere Medium das Internet. Das ist mittlerweile überall verfügbar, egal ob mobil oder nicht mobil, und was ich haben möchte, ist eigentlich immer auf irgendeine Weise eine sichere Verbindung, in diesem Fall meistens zur Firmenzentrale, um meine Anwendungen des eigenen Unternehmens erreichen zu können.

Da gibt’s verschiedene Ausprägungen, je nachdem, wie die Anforderungen sind. Das kann sein, dass ich nur mit einem mobilen Endgerät bestimmte Anwendungen erreichen möchte. Es kann aber auch notwendig sein, dass ich vielleicht sogar von mehreren Geräten aus eine sichere Netzwerkverbindung ins Unternehmensnetz brauche. Typischer Anwendungsfall wäre da, ich habe zuhause nicht nur das übliche Firmen-Notebook, sondern auch ein Festnetztelefon, das ich aus der Firma mit nach Hause nehme, dann habe ich den Fall, dass ich eine Kopplung mit meinem kleinen Firmennetz zuhause, das aus diesen beiden Geräten besteht, in die Firma brauche. Es sind da ganz verschiedene Konstellationen möglich.

Grundgedanke ist immer, dass ich eine Verbindung haben möchte, die die Grundziele der Informationssicherheit – Vertraulichkeit, Verfügbarkeit und Integrität – im Blick behält. Ich möchte

nicht, dass irgendwer die Daten, wenn sie unterwegs sind über das unsichere Medium, abhören kann – Vertraulichkeit. Ich möchte nicht, dass sie unterwegs verfälscht werden – Integrität – und ich möchte, dass, wenn ich eine Verbindung herstelle, natürlich auch die Daten, die auf der einen Seite gesendet werden, auf der anderen Seite ankommen, d.h. die Verfügbarkeit muss gegeben sein.

Die ist natürlich beim Thema VPN immer abhängig davon, wie verfügbar die Internetverbindung an beiden Enden ist. In der Firmenzentrale muss ich ein möglichst verfügbares Netz haben mit Internetzugang und am mobilen Arbeitsplatz, wo auch immer, muss ich natürlich auch eine verfügbare Internetverbindung haben. Das sind aber auch schon die einzigen Voraussetzungen, die wir brauchen, um die VPN-Verbindungen, so wie sie der Kunde braucht, herzustellen. Das ist ja genauso wie die Telefonie in ihren ganzen Ausprägungen unsere Kernkompetenz, also da können wir wirklich anfangen bei den Anforderungen, die bestehen, und Lösungen in ganz verschiedenen Ausprägungen bauen.

Michael Schneider: Das heißt also, wenn ich ein sicheres Home Office haben möchte, ein sicheres Umfeld für meine Mitarbeiter, dann muss ich auf jeden Fall so einen VPN-Tunnel herstellen, um möglichst sicher kommunizieren zu können mit dem entsprechenden Mitarbeiter oder umgekehrt der Mitarbeiter mit dem Firmennetzwerk. Das gilt sowohl für die Telefonie als auch für den Datenfluss übers Notebook, über meine Anwendung.

5 Wie kann ich als Arbeitgeber die Performance sicherstellen?

Michael Schneider: Als Administrator: Wie kann ich denn sicherstellen, dass ich für meine Mitarbeiter, die dann im Home Office sind, auch genug Performance zur Verfügung stellen kann? Habe ich die Möglichkeit, an meiner Firewall irgendwelche Mechanismen einzustellen, oder was muss ich überprüfen, um überhaupt feststellen zu können, dass die Kapazität ausreicht?

Sebastian Pfeiffer: Da können wir sicherlich bei helfen, wenn’s Unsicherheiten gibt. Wenn es eine klassische VPN-Verbindung ist, die also auf der firmenzentralen Seite ein klassisches VPN-Gateway hat, das ist eine ganz übliche Variante, dann hab ich an dieser Stelle natürlich Überprüfungsmöglichkeiten. Ich kann also in der Planungsphase gucken: Um wie viele Mitarbeiter geht es eigentlich? Um welche Anwendungen geht es? Und hab da schon mal eine Planungsgrundlage. Wenn es darum geht, im laufenden Betrieb nachzugucken, dann ist das zentrale VPN-Gateway genau die Informationsquelle, die ich brauche, um an die Informationen zu kommen.

6 Wie kann ich den Mitarbeiter optimal mit dem Firmennetzwerk und der Telefonanlage verbinden und so seine Erreichbarkeit sicherstellen?

Michael Schneider: Heiko, nochmal zu dir: Du hattest ja verschiedene Möglichkeiten vorgestellt, wie ich die Telefonie einrichten kann, um den Mitarbeiter mit dem Firmennetzwerk, mit der Firmen-TK-Anlage verbinden zu können. Was würdest du denn favorisieren? Was wäre dein optimaler Weg, um den Mitarbeiter dort anzubinden?

Heiko Bulmahn: Also wenn ich den Funktionsumfang von der Firma erhalten möchte, den die Mitarbeiter gewohnt sind, gerade bei speziellen Anwendungen, macht es am meisten Sinn, das über einen VPN-Zugang zu machen. Am sinnvollsten dann noch über ein Softphone, das ja eben den Sinn

hat, dass man das auf dem Notebook oder als App auf dem Handy installieren kann und somit komplett mobil ist, ohne ein Hardware-Telefon aus der Firma immer durch die Gegend schleppen zu müssen.

Wovon ich abraten würde, ist, den Mitarbeiter nur mit seinem privaten Telefon auf die Kunden loszulassen im Sinne einer einfachen Anrufumleitung – das ist eher ein Notbehelf.

In der Mitte würde dann die Lösung liegen, dass man für die Mitarbeiter eine Art Remote Worker Zustand einrichtet, wo ich also das Telefon zuhause nutzen kann, aber die TK-Anlage quasi den Mitarbeiter zuhause anruft und er auf diesem Weg simuliert im Firmennetzwerk drin ist. Das Ganze läuft dann über Telefonie, da brauche ich nicht unbedingt einen VPN-Zugang für, wenn ich das normale Festnetztelefon von den Mitarbeitern nehme. Der Funktionsumfang ist nicht ganz so gut von den meisten Herstellern, wie ich es aus der Firma gewohnt bin, aber ich sag mal für 50-60% reicht das sicherlich aus.

Aber ich kann sowas von vornherein ausschließen, wenn ich beispielsweise im Call-Center-Bereich arbeite, denn da ist es ja oft so, dass auch Statistiken geführt werden – durchschnittliche Gesprächsdauer; wie lange dauert es, bis einer rangeht usw. – und dafür brauche ich dann in der Regel auch User mit VPN-Zugang. Also da würden die anderen beiden einfachen Varianten ausscheiden in den meisten Fällen.

7 Warum sollte der Mitarbeiter nur über die Firmen-Rufnummer kommunizieren?

Michael Schneider: Also du würdest ganz klar dahin tendieren und sagen: Der Mitarbeiter muss über seine Firmennummer erreichbar sein und das kann sichergestellt werden entweder über ein Softphone, was eigentlich die optimale Variante ist als Software-Tool auf dem Notebook, ergänzt vielleicht durch eine App auf dem Smartphone, um auch dort dem Anrufempfänger gegenüber zu simulieren „Das ist die Nummer desjenigen, der auch dann im Büro so erreichbar wäre“?

Heiko Bulmahn: Absolut. Es macht allein schon aus dem Grund Sinn, dass meine Geschäftskontakte mich entsprechend in ihren Kontakten ja auch mit der Firmen-Rufnummer eingerichtet haben, weil ich diese zum Beispiel auch in meiner Signatur verbreite. Stell dir mal vor, ich als Mitarbeiter habe einen Telefon-Termin mit dem Kunden vereinbart, rufe aber mit einer ihm nicht bekannten und eingespeicherten Nummer an. Im schlimmsten Fall geht der Kunde dann gar nicht ans Telefon, weil er sich den Zeit-Slot ja für den Telefon-Termin freihalten will. Es kann ein Haufen Situationen entstehen, die zu Kommunikations-Missverständnissen führen, und das richtet oftmals mehr Chaos an, als dass es Nutzen schafft.

Auch der Arbeitgeber hat ja üblicherweise ein Interesse daran, dass die Mitarbeiter unter seinem Firmennamen auftreten. Worst Case könnte es zum Beispiel überspitzt sein, dass Mitarbeiter mit einer Privatnummer den Kunden anrufen, die eine andere Vorwahl hat als die Stadt, in der man vielleicht dem Kunden aber vertraglich einen Service-Stützpunkt zugesichert hat. Dieses Risiko will ja keiner eingehen, nur weil der Mitarbeiter mal mobil arbeitet. Klar bringt es auch ein Stück weit noch mehr Flexibilität, wenn ich als Mitarbeiter die Privatnummer nutze, aber es bringt eben auch viele Nachteile mit sich, die es zu berücksichtigen gilt.

Und noch ein weiterer Aspekt daran, Stichwort Fachkräftemangel: Der ein oder andere potenzielle Konkurrent kann so natürlich auch private Kontaktdaten der Mitarbeiter sammeln, um gute Mitarbeiter abfischen zu können. Das sind alles Dinge, die man dabei im Hinterkopf haben sollte.

Michael Schneider: Ich glaube, ein ganz großer Vorteil dieser Lösung ist auch die Rufumleitung. Ich kann mir auch gut vorstellen, gerade in dieser Corona-Zeit, wenn ein Mitarbeiter erkrankt ist im Home Office, habe ich als Unternehmen jederzeit die Chance, eine Rufumleitung herstellen zu können. Dass also der Mitarbeiter durch einen anderen vertreten wird, die Rufnummer umgeleitet wird über die zentrale TK-Anlage, die Möglichkeit hätte ich ja beispielsweise über die Privatnummer nicht.

Heiko Bulmahn: Genau, der potenzielle Geschäftspartner weiß ja gar nicht, dass der Mitarbeiter krank ist, und würde diesen dann vielleicht unter der privaten Nummer anrufen und hört dann, dass der Mitarbeiter krank ist oder im Urlaub, und dann geht die Diskussion los, wer jetzt zuständig ist usw. Das sind die ganzen Thematiken, die ich von Vornherein vermeiden kann, wenn ich das gleich professionell richtig einrichte.

Sebastian Pfeiffer: Wir dürfen ja auch ein Thema nicht außer Acht lassen: Dieses „Der Kunde sieht die private Telefonnummer des Mitarbeiters“ ist auch ein Datenschutzthema. Als Mitarbeiter möchte ich vielleicht gar nicht, dass irgendein Kunde meine private Telefonnummer sieht. Der eine fühlt sich vielleicht nur unwohl damit, der andere vermeidet es vielleicht sogar, überhaupt zu telefonieren, was wiederum nicht im Sinne des Unternehmens ist.

8 Wie kann ich als Administrator die Sicherheit und Performance der Unternehmens-IT-Infrastruktur überprüfen?

Michael Schneider: Sebastian, was mich nochmal interessiert: Was könnte ich denn als Administrator eines Unternehmens tun, um im Vorfeld zu eruieren, ob meine Infrastruktur im Bereich Security ausreichend ist für solch einen „Katastrophen-Fall“ wie jetzt die Corona-Zeit, um ganz plötzlich reagieren zu können, wenn alle Mitarbeiter im Home Office sitzen, dass mir nicht meine ganze Infrastruktur im Unternehmen wegbricht und keine Performance mehr bietet?

Sebastian Pfeiffer: Das erste ist das zentrale VPN-Gateway, die Firewall ist das meistens gleichzeitig auch, da kann ich erstmal gucken, zu wie vielen gleichzeitigen VPN-Verbindungen ist das Gerät überhaupt in der Lage. Das kann eine physische Appliance sein, die irgendwo steht, das kann eine virtuelle Appliance sein, der Mechanismus ist derselbe.

Ich muss in den Eckdaten gucken, wie viele gleichzeitige VPN-Verbindungen unterstützt das jeweilige Modell und muss ich da vielleicht noch was lizensieren, das ist von Hersteller zu Hersteller ganz unterschiedlich. Und wie viele Mitarbeiter betrifft das potenziell? Da kann ich schon mal vergleichen: Hab ich zum Beispiel 200 mögliche gleichzeitige Verbindungen zur Verfügung, aber nur 150 Mitarbeiter insgesamt, dann bin ich auf der sicheren Seite, was das angeht.

Ein anderer wichtiger Punkt ist, zu überprüfen, ob denn eigentlich die Bandbreite der Internet-Anbindung auch dafür ausreichend ist. Und da ist es schon nicht mehr ganz so einfach, da muss man nämlich gucken, wie viel Bandbreite verbraucht denn so eine typische Verbindung eines Mitarbeiters? Das kann man nicht ganz so schnell beantworten, da muss man sich vielleicht auch

einfach mal die Situation mit – und wenn's nur wenige Mitarbeiter sind, die da arbeiten – angucken: Wie viel Bandbreite verbrauchen die? Und dann kann man hochrechnen, wenn's noch einige mehr sind, passt das noch oder sind wir jetzt schon an der Grenze?

Ganz wichtig wird das natürlich, wenn's um das Thema Telefonie geht, also wenn ich Telefonie zusammen mit den Daten über die VPN-Verbindung übertragen will, dann ist es natürlich extrem wichtig, dass möglichst eine Reserve da ist in der Bandbreite, denn ansonsten besteht die Gefahr, dass die Echtzeit-Daten der Telefonie nicht mehr sauber übertragen werden.

9 Welche Risiken birgt eine schlechte Netzwerkverbindung für die Telefonie über VPN und wie kann ich diese vermeiden?

Michael Schneider: Das heißt, dann könnte es auch zu Verbindungsabbrüchen kommen, gerade im Bereich der Telefonie?

Sebastian Pfeiffer: Genau, es kann zu Verbindungsabbrüchen kommen, wobei das schon der Extremfall ist. Was man viel eher bemerkt, ist, dass es Gesprächs-Aussetzer gibt, die Verzögerung wechselt – mal habe ich eine größere Verzögerung, mal kriege ich Gesprächsfetzen ein bisschen früher – das sind dann alles so Phänomene, wo zwei Dinge erstmal zusammenkommen müssen: Einmal gibt es an irgendeiner Stelle des Übertragungsweges einen Engpass, und es gibt keine Bevorzugung für die Echtzeitdaten.

Wenn das Netz komplett von mir selbst kontrolliert wird, dann kann ich an jedem Punkt dafür sorgen, dass die Daten, die mir wichtig sind – die Echtzeitdaten, die Telefoniedaten – auch bevorzugt werden. Denn wenn ich noch ein bisschen länger auf einen Download warte, ist das nicht so schlimm, ich muss aber dafür sorgen, dass die Telefoniedaten möglichst schnell übertragen werden. Das kann ich aber nicht überall im Internet machen. Ich muss also dafür sorgen, dass die Punkte, die ich selbst kontrollieren kann, die Anbindung zum Internet und das VPN-Gateway, entsprechend von der Performance her genug Reserven haben und ich muss eben dort dafür sorgen, dass, wenn's zu einem Engpasse kommt, die Echtzeitdaten bevorzugt werden.

Michael Schneider: Das heißt Stichwort „Quality of Service?".

Sebastian Pfeiffer: Genau, oder zu deutsch „Priorisierung".

10 Wie kann ich verschlüsselte Verbindungen für Datenverkehr und Telefonie sicherstellen – und muss ich das überhaupt?

Michael Schneider: Ein weiteres Thema, das viele Kunden umgetrieben hat, ist das Thema Verschlüsselung. Wie kann ich denn sicherstellen, dass ich verschlüsselte Verbindungen herstellen kann ins Unternehmen? Ich hab da noch so im Hinterkopf beispielsweise SSL, aber sicher gibt's da auch noch andere Standards im Bereich der Verschlüsselung. Kann ich diese Verschlüsselung nicht nur für den Datenverkehr, sondern auch für die Telefonie nutzen?

Sebastian Pfeiffer: Klar, das ist sogar sinnvoll. Also wenn wir über das Thema Softphone und ähnliche Dinge wie ein dienstliches Telefon, das ich als Mitarbeiter mit nach Hause nehme, nachdenken, dann ist es für manche Unternehmen sogar gesetzlich vorgeschrieben, dass die Gesprächsdaten verschlüsselt werden. Und auch wenn's nicht vorgeschrieben ist, ist es gängige Praxis. Niemand möchte gerne seine Telefongespräche unverschlüsselt übers Internet schicken, denn man weiß nicht, wer dort irgendwo die Leitung anzapft und irgendwelche Dinge versucht mitzuhören.

Michael Schneider: Heiko, da stellt sich mir nochmal die Frage: Verschlüsselung im Bereich Telefonie, wo fängt sie an, wo hört sie auf? Also wenn ich jetzt im Home Office sitze, da kann ich mir das noch gut vorstellen, die Verschlüsselung über das Internet über VPN bis in meine TK-Anlage, aber da hört die doch eigentlich auf, oder? Also ich hab ja keine Verschlüsselung bis zu meinem Gesprächspartner am anderen Ende der Leitung oder sehe ich das falsch?

Heiko Bulmahn: Das kommt drauf an. Also wir müssen da unterscheiden zwischen Firmennetzen, also wo ich innerhalb einer Firma eine Telefonanlage habe, die kann innerhalb ihres Bereiches komplett verschlüsselt sein, auch was die Gespräche betrifft. Das gibt es sowohl für klassische System-Schnittstellen, da werden dann Verschlüsselungsboxen eingesetzt, die an zentralen Stellen platziert werden, sodass erstmal die Sprachkommunikation innerhalb des Unternehmens komplett verschlüsselt werden kann. Bei den IP-Geräten hingegen ist es so, dass die Geräte es teilweise selber machen, teilweise mit Standard-Modulen, teilweise auch über eine proprietäre Verschlüsselung, je nach Hersteller. Der Mitarbeiter, der mit einem IP-Phone über VPN ins Firmennetz reingeht aus dem Home Office, kann also in der Tat die Verschlüsselung mitnutzen.

Wenn ich jetzt aber aus dem Unternehmen heraus eine x-beliebige Person anrufe, dann hört es in der Tat in vielen Fällen auf, es sei denn ich hab noch zusätzliches Equipment, womit ich wirklich eine Ende-zu-Ende-Verschlüsselung mache. Dazu muss aber dann auch die Gegenseite mit in der Lage sein und die gleiche Technik einsetzen. Ich selbst auf meiner Seite habe einen gewissen Einfluss auf das, was bei mir passiert, und genauso hat das Gegenüber, der Anrufempfänger, auf seiner Seite den jeweiligen Einfluss, aber dazwischen hat man ja eigentlich keine Möglichkeit, irgendwas zu kontrollieren. Und dafür gibt es Gerätschaften für eine Ende-zu-Ende-Verschlüsselung, und dann kann ich auch sowas mit angemessenem Aufwand entsprechend verschlüsseln, sodass ich auch für solche Sachen eine gesicherte Kommunikation habe.

Das wird in gewissen Unternehmensbereichen auch gemacht. Da hat Sebastian vorhin ja auch schon gesagt, dass es Bereiche gibt, in denen das vorgeschrieben ist, und Bereiche, in denen Unternehmen das von sich aus machen, um sicherzugehen, dass Geschäftsgeheimnisse usw. nicht verteilt werden. Wiederum andere Firmen, die mit nicht so sensiblen Daten handeln, oder bei denen es aus deren Sicht nicht notwendig ist, legen in der Regel kein Augenmerk darauf, weil es natürlich auch Geld kostet, wenn ich da was verschlüssele.

Aber grundsätzlich ist eine solche Verschlüsselung möglich, und ich sage mal runtergebrochen: Je höher der Aufwand ist, desto höher ist auch die Sicherheitsstufe.

Michael Schneider: Ok, super, ich denke, für heute haben wir genug Input bekommen, den wir jetzt erstmal verarbeiten müssen. Vielen Dank für eure kompetenten Antworten! Ich hoffe, wir konnten heute einige Fragen klären zum Thema sicheres Home Office.

Ich möchte an der Stelle nochmal hinweisen auf unsere nächste Folge, in der es auch wieder um das sichere Home Office gehen wird. Denn wir haben jetzt alle in dieser Phase gemerkt, dass man auch

das Thema Awareness auf dem Schirm haben muss, denn jeder Mitarbeiter, der sein Notebook zuhause aufklappt, stellt den Inhalt des Notebooks auch potenziell anderen Menschen zur Verfügung, d.h. erstmal seinem familiären Umfeld, seinen Kindern, seiner Frau, seiner Verwandtschaft, Bekanntschaft, und auch das sollte daher ein Thema sein, das wir dann im nächsten Podcast näher beleuchten wollen.

Vielen Dank!