Homeoffice – aber richtig

Die IT-Infrastruktur muss an die neue Anforderung angepasst werden

Kai-Oliver Detken

Die Corona-Pandemie hat das Arbeitsleben in Deutschland nachhaltig verändert. Hatten früher die Unternehmen ihren Beschäftigten in Ausnahmefällen mobiles Arbeiten außerhalb der Firma gestattet, so ist dies jetzt oftmals der Regelfall. Ein komplettes Zurück in die Unternehmen wird es nach Ansicht einiger Experten wohl nicht mehr geben. Daher wird es immer wichtiger, die IT-Infrastruktur auch auf diese neue Anforderung anzupassen. So litt bisher die IT-Sicherheit unter der Homeoffice-Nutzung, und auch die telefonische Anbindung war teilweise nur sehr umständlich machbar.

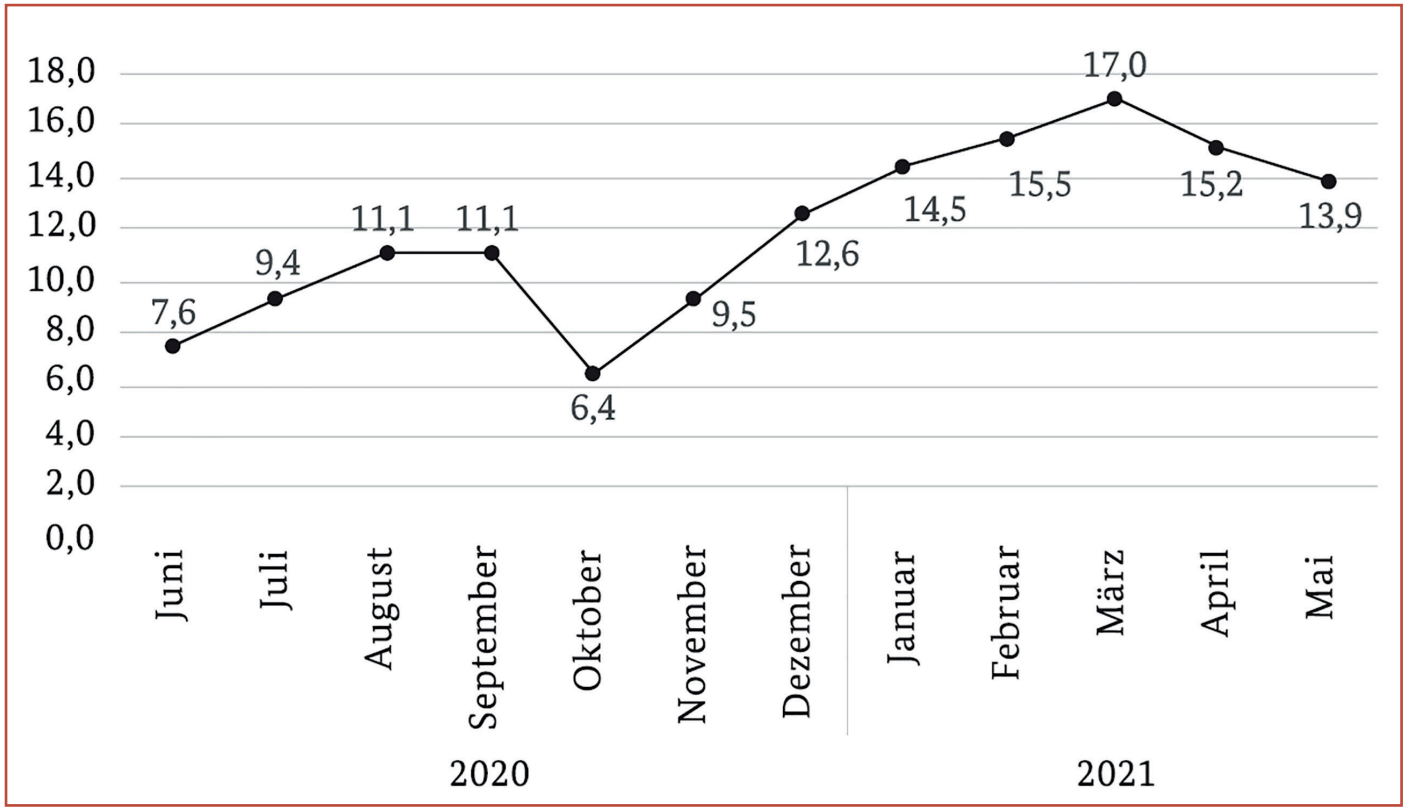
Allen Unternehmen sollte bewusst sein, dass es keine fehlerfreie Software gibt und ihre Netze und Systeme auch im Homeoffice permanent geschützt werden müssen (Bild: Mariimaccarii, pixabay)

Mobiles Arbeiten war bereits vor Corona bei vielen IT-Unternehmen standardmäßig möglich. Ob auf Geschäftsreisen, beim Kunden oder nach Feierabend zu Hause, per VPN-Anbindung konnte schnell und flexibel mit dem Geschäftslaptop auf die Unternehmensdaten zugegriffen werden. Deshalb war diese Branche auch auf den Lockdown in Deutschland wohl am besten vorbereitet und konnte nahezu nahtlos weiterarbeiten. Schwieriger ist es hingegen bei Firmen oder Behörden, die normalerweise die Anwesenheit der Arbeitnehmer voraussetzen. Durch die plötzliche Homeoffice-Pflicht waren diese Mitarbeiter plötzlich von ihrem Arbeitsplatz abgeschnitten, waren telefonisch nicht mehr erreichbar und mussten privates IT-Equipment nutzen, um von zu Hause aus arbeiten zu können. Zusätzlich wurde dadurch eine neue Bedrohungslage geschaffen, da die Unternehmen und Behörden auf einmal den VPN-Zugriff über fremdes Privat-Equipment zulassen mussten.

Hinzu kam, dass dienstliche Dokumente mit privaten Daten vermischt wurden und dass die IT-Administrationen keinen Zugriff auf das private Equipment hatten, dementsprechend auch keine Antivirensoftware oder Firewall-Funktionalität aktivieren konnten. Es kam daher im Jahr 2020 zu einer Flut von Laptop- und Terminal-Server-Bestellungen. Während die Laptop-Fraktion von der Installation der IT-Administratoren abhängig war, konnte man bei einer Terminal-Server-Lösung auch das private bereits einsatzbereite Equipment nutzen, um über RDP-Verbindung auf die Unternehmensdaten zuzugreifen. Die eigentlichen Daten verbleiben dabei in der Firma.

Das Problem der telefonischen Erreichbarkeit ist damit aber noch nicht gelöst. Und der Datenschutz spielt ebenfalls noch eine wichtige Rolle bei der Entscheidung, wie mobiles Arbeiten realisiert werden soll.

Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen



Angespannte IT-Sicherheitslage

Jedes Jahr veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Lagebericht zur IT-Sicherheit. Im aktuellen Bericht stuft das BSI die Lage in Deutschland als bedenklich ein, was nicht nur an der Anzahl neuer Schadprogrammvarianten (siehe Bild 1) und Sicherheitsvorfälle liegt, sondern auch an neuen, angepassten Angriffsmethoden, die die massenhafte Ausnutzung schwerwiegender Software-Schwachstellen ermöglichen. Schwachstellen in IT-Produkten ermöglichen diese neuen Angriffswege, die besonders gravierend sind, wenn diese Produkte einen großen Verbreitungsgrad aufweisen. Dies wurde besonders bei zwei Fällen deutlich: MS-Exchange-Bugs und Log4j. Exemplarisch schauen wir uns einmal den erstgenannten an.

Im März 2021 veröffentlichte Microsoft ein außerplanmäßiges Sicherheitsupdate für das Produkt MS-Exchange-Server. Das Update sollte vier kritische Schwachstellen beheben, die in Kombination gezielte Angriffe auf ein Unternehmensnetz ermöglichten. Eine Schwachstelle erleichtert es beispielsweise Angreifern, sich durch das Senden speziell formulierter http-Anfragen auf dem MS-Exchange-Server zu authentifizieren. Anschließend konnte durch das Ausnutzen einer weiteren Schwachstelle ein beliebiger Programmcode mit administrativen Zugriffsrechten ausgeführt werden. Dadurch konnten Angreifer auf den Servern Hintertüren in Form von sog. Web-Shells einschleusen. Selbst nach der Installation der Sicherheitsupdates von Microsoft blieben diese bestehen, so dass Hacker weiterhin den vollen Zugriff auf die kompromittierten Server hatten. So ließen sich die E-Mails auf dem MS-Exchange-Server ausspähen oder weitere Schadprogramme wie Ransomware auf das Unternehmensnetz ausrollen.

Zum Zeitpunkt der Bekanntmachung von Microsoft waren 98 % der Systeme in Deutschland betroffen. Kurze Zeit später wurde das Internet großflächig nach verwundbaren Systemen gescannt. Alle diese Serversysteme waren einem extrem hohen Risiko ausgesetzt, mit Schadsoftware infiziert zu werden. Daher mussten auch bereits gepatchte Systeme auf zuvor erfolgte Angriffe hin untersucht werden. Problematisch war dabei, dass viele Systeme auf veralteten Versionsständen basierten, die auch nicht mehr gepatcht werden konnten. In vielen Fällen blieb daher nur noch die Neuinstallation der MS-Exchange-Umgebung. Zwei Monate später waren zwar durch das schnelle Reagieren des BSI nur noch 9 % der Systeme betroffen, aber in den ersten Tagen der Bekanntmachung hatten bereits tausende von Firmen in Deutschland mit ernsthaften Auswirkungen dieser Schwachstelle zu kämpfen.

Bild 1: Der aktuelle Bericht des BSI weist eine bedenklich hohe Zahl neuer Schadprogrammvarianten aus (Anzahl in Mio.) (Quelle: BSI-Auswertung von Rohdaten des Instituts AV Test GmbH)

Den Unternehmen sollte daher bewusst sein, dass es keine fehlerfreie Software gibt und ihre Netze und Systeme auch im Homeoffice permanent geschützt werden müssen. So kamen die Angreifer auch nur auf die MS-Exchange-Systeme, weil diese per Internet von außen direkt erreichbar waren, um Push-Nachrichten an Mitarbeiter verschicken zu können. Wenn man diese

Systeme nur per VPN-Einwahl zugänglich gemacht hätte, wäre das Risiko einer Schwachstelle stark reduziert worden. Dies ist für die meisten IT-Administratoren oder Anwender aber anscheinend zu umständlich, weshalb auf ein höheres Niveau der IT-Sicherheit bewusst verzichtet wurde.

Absichern des Arbeitsplatzes

Grundsätzlich ist das Homeoffice schlechter abgesichert, als das Firmennetz und daher prädestiniert für ein Hacker-Einfallstor. Hinzu kommt, dass man sich das Heimnetz mit anderen Teilnehmern (wie z.B. den eigenen Kindern) teilt, die nicht zum Unternehmen gehören und sich auch nicht an dessen Sicherheitsrichtlinien halten. In den meisten Fällen sind die Geräte auch noch über ein Wireless LAN miteinander verbunden, das nur einfach abgesichert und auch beim Nachbarn noch erreichbar ist. Wird nun ein Laptop des aktiven Internetnachwuchses gehackt oder ist auf einmal Mitglied in einem Botnet, wird auch der Unternehmensrechner in Mitleidenschaft gezogen. In diesem Fall schützt auch keine sichere VPN-Verbindung mehr das Unternehmen, da sich ein unsicherer Rechner im Heimnetz befindet, der nun den VPN-Tunnel direkt ausnutzen kann.

Es sollten daher einige Grundregeln beherzigt werden, damit das sichere Arbeiten von zu Hause aus gelingen kann:

- Falls möglich sollte dem Mitarbeiter ein Firmen-Laptop gestellt werden, der mit unternehmensspezifischer Sicherungssoftware ausgeliefert wird.
- Private und personenbezogene Daten sollten auf diesem Laptop nicht enthalten sein. Dies kommt auch dem Datenschutz entgegen.
- Als zweite Variante könnte eine verschlüsselte Festplatte, in einem Desktop-PC mit zweitem Boot-Betriebssystem, genutzt werden. Dies geht heutzutage auch von einem USB-Stick aus.
- Als dritte Variante könnte für ein privates Endgerät ein RDP-Zugang (Remote Desktop Protocol) für einen Terminalserver zum Einsatz kommen.
- Der Datenaustausch darf nur über gesicherte Kanäle (z.B. VPN, Terminalzugang) mit dem Unternehmen erfolgen.
- Der Virenschutz und Sicherheitsupdates müssen auf dem Homeoffice-Rechner auf dem neuesten Stand gehalten werden, auch bei Nutzung eines Remote-Terminal-Zugangs. Der zentrale Policy-/Antivirensserver muss daher auch die Homeoffice-Rechner erreichen können.
- Der Zugriff auf den Laptop oder Desktop-PC muss über eine Desktop-Firewall zusätzlich gesichert werden, auch um sich vor anderen Teilnehmern im Heimnetz schützen zu können.
- Ein Datensicherungskonzept sollte für mobiles Arbeiten existieren. D.h., es sollten möglichst nur auf dem Firmenserver Daten gespeichert werden, damit diese im täglichen Backup landen.

Viele Unternehmen nutzen auch Cloud-Lösungen für die Homeoffice-Anbindungen aus, da sie nicht so schnell sichere VPN-Verbindungen umsetzen konnten oder sowieso bereits Teildienste ausgelagert hatten. Die Daten liegen damit in einer gesicherten Umgebung und können von allen Mitarbeitern bearbeitet werden. Dies muss nicht unbedingt durch eine Public Cloud umgesetzt werden, sondern ist oftmals auch durch eine private Cloud im eigenen Rechenzentrum möglich, was auch dem Datenschutz entgegenkommt.

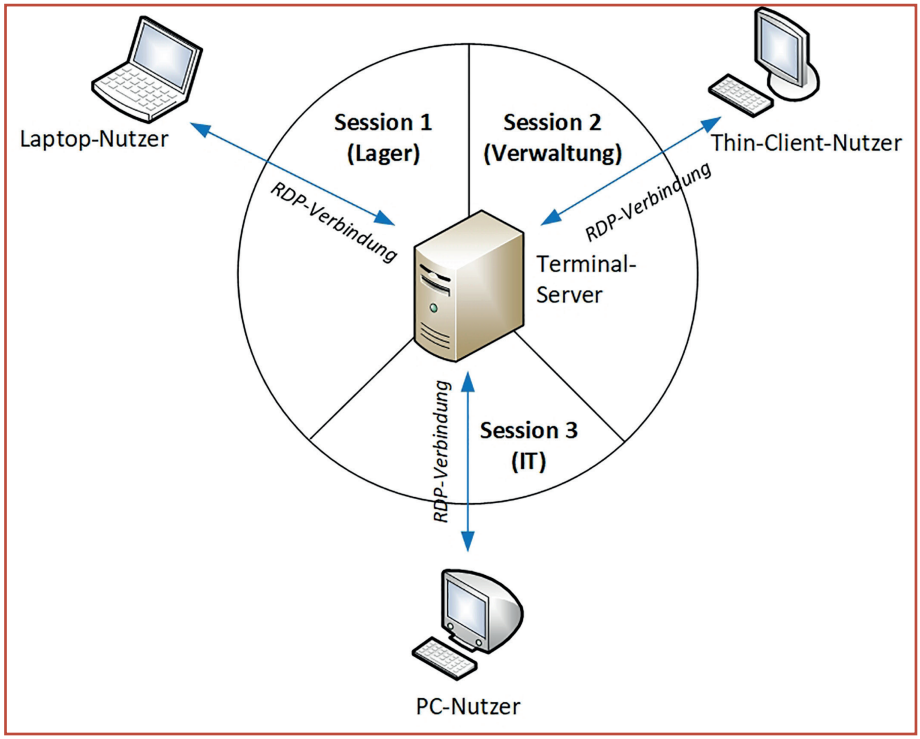


Bild 2: Sessionbasierte RDP-Zugänge auf zentral gehostetem Terminalserver, der auch das aktuelle Windows-Betriebssystem für den Client bereitstellt. Die Clients im Homeoffice brauchen so keine Festplatte mehr

Als Beispiel für eine Terminalanbindung können namhafte Hersteller wie Citrix und Microsoft exemplarisch genannt werden. Aber es lassen sich auch Linux-Lösungen mit Microsoft kombinieren, indem man beispielsweise ein angepasstes PXE-Boot-Image für Linux nutzt, das nur die nötigsten Programme besitzt. Dieses Image enthält dann auch einen RDP-Connection-Manager, in dem der Benutzer aus den vorhandenen Sitzungen verschiedene Unternehmensbereiche wie Lager, Verwaltung oder IT auswählen kann (siehe Bild 2). Anschließend kann direkt mit einem Windows-Terminalserver kommuniziert werden, der zentral gehostet wird und das aktuelle Windows-Betriebssystem für den

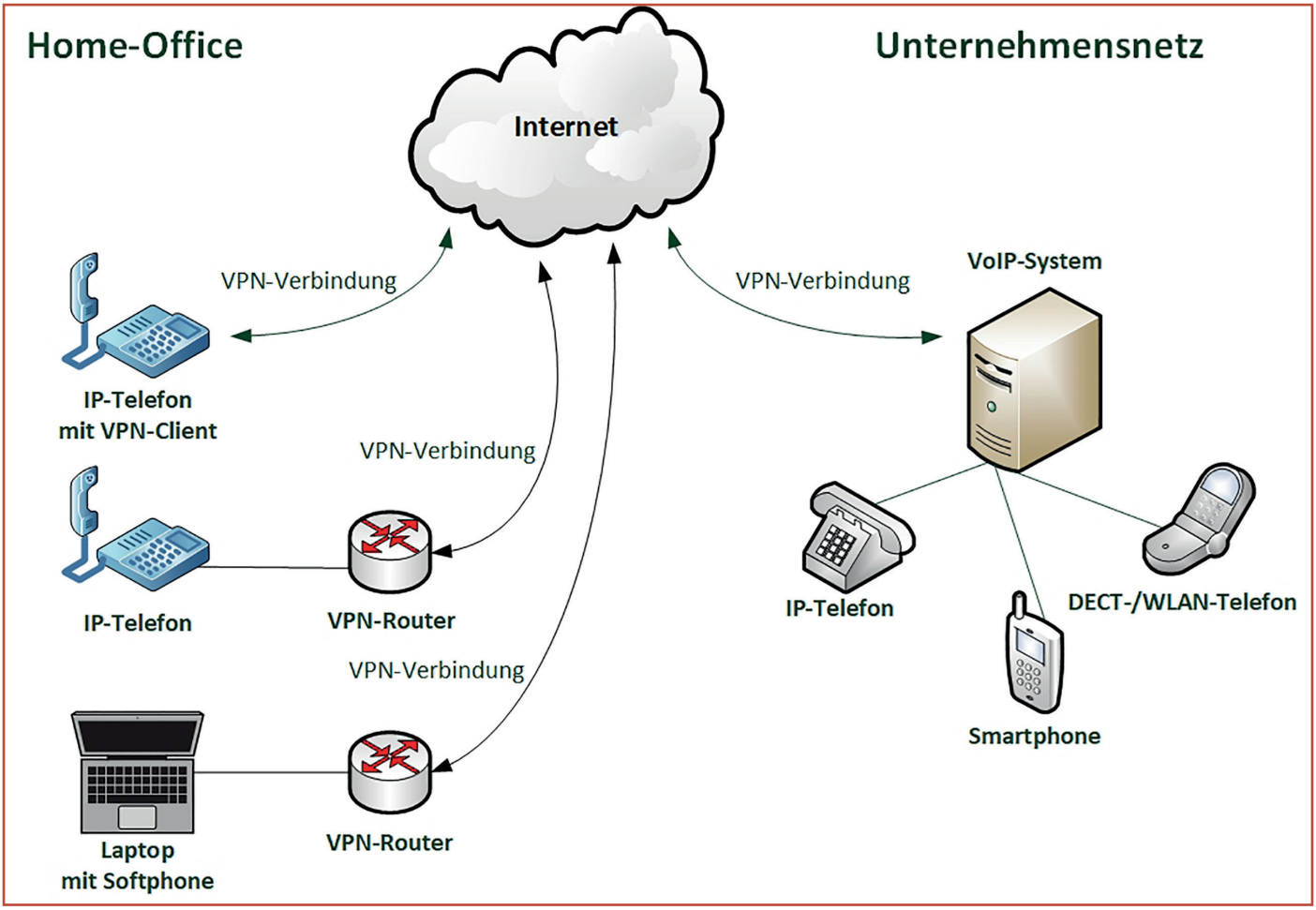


Bild 3: Die Telefonanbindung im Homeoffice kann bei Vorhandensein nativer VoIP-TK-Anlagen unterschiedlich realisiert werden. Hierbei wird bereits ein IP-Telefon im Homeoffice eingesetzt

Client bereitstellt. Da dies mittels Preboot Execution Environment (PXE) funktioniert, benötigen die Clients im Homeoffice keine Festplatte mehr. Die PXE-Images sind hingegen auf einem NAS-System verfügbar. Bei auftretenden Sicherheitslücken oder anderen notwendigen Updates wird einfach ein neues Image gebaut und verteilt. Beim nächsten Bootvorgang liegt dies dann automatisch dem Benutzer vor. Ein weiterer Vorteil dabei ist, dass auch ältere bzw. beliebige PC-Hardware so mit einem aktuellen Windows-Betriebssystem verwendet werden kann.

Telefonanbindung im Homeoffice

Bleibt noch die Telefonanbindung zu klären. Traditionelle (ISDN-) Telefonanlagen sind nur in der Lage, Weiterleitungen zu initiieren. Das heißt, man bekommt zwar durch externe Anrufe den entsprechenden Mitarbeiter ans Telefon, dieser kann aber nicht mit seiner Bürorufnummer zurückrufen. Falls das Unternehmen bereits in eine native VoIP-Anlage investiert hat, taucht dieses Problem nicht auf. ISDN-Anlagen oder aufgerüstete ISDN-Anlagen mit VoIP-Modulen sind aber oftmals nicht in der Lage, diesen Komfort zu unterstützen. Daher gab es aus Datenschutzgründen oftmals ein Problem bei den Rückrufen, da der Mitarbeiter seine private Nummer nicht verraten wollte.

Bei nativen VoIP-Telefonanlagen sind bereits im Homeoffice IP-Telefone im Einsatz. Dies kann, wie Bild 3 zeigt, unterschiedlich realisiert werden. Es können IP-Telefone über die bestehende VPN-Verbindung zur Firma an der VoIP-Anlage angemeldet werden, so dass der Mitarbeiter mit der gleichen Rufnummer intern und extern erreichbar bleibt. Falls kein VPN-Router verfügbar ist, lässt sich dies auch über ein IP-Telefon mit eingebautem VPN-Client lösen. Gleiches wäre natürlich auch über einen Laptop machbar, wenn ein Softphone Verwendung fände.

Fazit

Mobiles Arbeiten ist aus der modernen Arbeitswelt nicht mehr wegzudenken. War dies früher nur IT-affinen Firmen vorbehalten, die ihre Mitarbeiter mit Laptops und Mobiltelefonen standardmäßig ausstatten, waren in der Corona-Pandemie nun auch die eher traditionellen Firmen gefragt, dies umzusetzen. Dabei kamen aufgrund der geforderten Schnelligkeit der Umsetzung oftmals die IT-Sicherheit und der Datenschutz zu kurz. Es sollten im Homeoffice die gleichen Regeln wie im Unternehmen gelten.