Man darf sich nicht von der Sicherheitslösung im Home Office abhängig machen.

DIE CLOUD KOMMT INS BÜRO

DIE UNTERSCHÄTZTEN RISIKEN DES HOME OFFICE

von Michael Czwalina

Schweizer KMU sind das Rückgrat der Schweizer Wirtschaft. Sie machen in der Schweiz mehr als 99 Prozent der Unternehmen aus und stellen zwei Drittel aller Arbeitsplätze. Zahlreiche Unternehmen bewiesen in der Umstellungsphase zum Home Office zwar grosse Flexibilität, unterschätzten aber die damit verbundenen Risiken.

Der schlagartige Wechsel der Arbeitsumgebung von gut geschützten Firmen ins Home Office im Zeichen der Pandemie vergrösserte und vergrössert noch immer die Angriffsfläche für Hacker. Mitarbeiter im Home Office sind dauernd online und können von ihren Arbeitgebern nicht im gleichen Umfang geschützt werden wie im Büro.

Seit Beginn der Pandemie haben die Cyberangriffe auf KMU explosionsartig zugenommen. Bereits ein Viertel der Schweizer KMU hat einen Cyberangriff erlebt. Ein Drittel dieser Firmen hat dabei finanzielle Verluste und Reputationsschäden erlitten, jedes zehnte Unternehmen beklagt einen Verlust von Kundendaten, so die Experten von Digitalswitzerland. Die Arbeitsgruppe Cyber Risk beim Schweizerischen Versicherungsverband schätzt die jährlichen Kosten allein in der Schweiz auf über 9.5 Milliarden Schweizer Franken.

SICHERHEIT FÜR DAS HOME OFFICE

Sicherheitsbewusste Unternehmen können es nicht riskieren, ihre Netzsicherheit vom Wissen oder der technischen Ausstattung der Heim-Anwender abhängig zu machen. Um die notwendige IT-Sicherheit zu gewährleisten, braucht es angepasste Technologien. Mitarbeiter müssen in der Lage sein, sich hochsicher mit dem Firmennetzwerk zu verbinden, auf Daten zuzugreifen und sich mit Kollegen auszutauschen.

Hinzu kommt, dass das Arbeitsverhalten durch die «Digital Natives» schnellen Veränderungen ausgesetzt ist. In zehn Jahren stellen diese die Mehrheit der arbeitenden Bevölkerung. Die mit elektronischen Geräten und Online-Anwendungen aufgewachsenen jungen Menschen setzen vermehrt ihre bevorzugten privaten Geräte ein und forcieren damit den Druck auf die Unternehmen, neuste Technologien zu nutzen. Arbeitgeber mit einer klaren Strategie für dezentrales Arbeiten werden daher zunehmend attraktiver.

Eine Möglichkeit, das Arbeiten von zu Hause aus flexibler und sicherer zu gestalten, ist die Umstellung in die Cloud. Allerdings ist die Cloud per Definition zum Teilen gedacht, sodass es häufig ratsam bleibt, sensible Daten weiterhin intern oder in einer eigenen Private-Cloud-Lösung zu speichern.

Die Umstellung in die Cloud ist allerdings auch mit Aufwand verbunden und es gibt oft Unklarheiten, welche bestehenden On-Premises-Anwendungen in die Cloud migriert werden können. Viele KMU erkennen die Notwendigkeit, ihre IT-Landschaft zu modernisieren, scheuen allerdings den damit verbundenen Aufwand.

Ob nun Cloud oder nicht, Unternehmen brauchen sichere Lösungen, um vernetzt zusammenzuarbeiten und von überall auf die Daten zugreifen zu können. Doch welche Alternativen gibt es?

DER WEBCONNECTOR

Die neue Virtual-Gateway-Lösung namens Webconnector verbindet die Vorteile der Büro-Desktops mit den modernsten mobilen Cloud-Arbeitsweisen für die digitale Büro-Organisation. Um den Webconnector zu nutzen, brauchen Sie die bestehende Windows-EDV-Organisation nicht zu ändern.

Ob Tablett, Mac oder privater Windows-Desktop, der Webconnector ermöglicht dem Anwender, von jedem browserfähigen Endgerät aus auf seine Geräte im Büro zuzugreifen und darauf zu arbeiten. Mitarbeitende im Home Office können so bequem von ihrem Privatrechner oder von unterwegs mit Tablett oder Handy auf ihrem Geschäftsdesktop arbeiten, ohne diesen ständig mitführen zu müssen. Dank der integrierten Wake-on-LAN-Funktion kann der Rechner jederzeit aus der Ferne gestartet oder heruntergefahren werden.

IM GESCHÜTZTEN FIRMENNETZWERK

Für die Unternehmen bedeutet der Einsatz des Webconnectors ein grosses Mehr an Sicherheit: Da die Home-Office-Anwender ihren Firmendesktop nicht nach Hause mitnehmen, sondern im geschützten Firmennetzwerk belassen, reduziert sich das Risiko, dass das Netzwerk mit Viren oder Ransomware infiziert wird, deutlich.

Der Zugriff erfolgt über eine sichere https-Verbindung mit TLS-Verschlüsselung (Transport Layer Security). Es handelt sich um eine direkte Verbindung ohne zentrale fremde Vermittlungsserver. Authentifiziert wird mittels 2FA-Handy-App (Zwei-Faktor-Authentifizierungsapp).

Der integrierte USB-Gateway ermöglicht es, USB-Geräte lokal anzuschliessen und über eine RDP-Verbindung auf dem Remote Device zu verwenden. Dadurch ergeben sich eine Vielzahl neuer Nutzungsmöglichkeiten, zum Beispiel die Smart-Card-Authentifizierung als weitere Sicherheitsebene für zu Hause. Durch die 30-FPS-Übertragungsrate ist auch die Remote-Arbeit an Multimediainhalten möglich.

Neben dem RDP-Protokoll (Remotedesktop-Verbindung) unterstützt der Webconnector auch Verbindungen per VNC, SSH, Telnet oder Kubernets im Browser. Er macht den Nutzer unabhängig vom Betriebssystem. Dieser kann sich somit auf seine Arbeit anstatt auf die Kompatibilität von Systemen konzentrieren.

WIE ERHALTE ICH DEN WEBCONNECTOR?

Die Webconnector-Lösung wird im Frühjahr 2022 offiziell lanciert und in der Schweiz über die vOffice CH AG lizenziert. Das Produkt kann bereits ab Dezember 2021 über www.webconnector.pro oder unter www.cc-it.cloud vorbestellt werden.

MICHAEL CZWALINA

ist Partner bei der
CC Czwalina Consulting AG.

www.czwalinaconsulting.com