Greenbone

Sicher im Homeoffice

[09.09.2020] Allein ein VPN-Zugang bietet für das Homeoffice zu wenig Schutz – ein Umstand, der Behörden und Unternehmen während der Corona-Pandemie stark beschäftigt hat. Für die sichere Arbeit von zu Hause aus ist ein starkes Schwachstellen-Management unabdingbar.

Nur dank schnell eingeführter Homeoffice-Lösungen konnten zu Beginn der Corona-Pandemie viele Unternehmen und Behörden den Betrieb aufrechterhalten und gleichzeitig ihre Mitarbeiter schützen. Das beschreibt Elmar Geese, COO bei Greenbone, in einem Kommentar über das sichere Arbeiten im Homeoffice. Allerdings bleibe fraglich, ob der Fernzugriff etwa auf das Firmennetzwerk überall die notwendige Vertraulichkeit, Verfügbarkeit und Integrität gewährleistet. Die Sicherheit des Homeoffice-Konzepts gehöre in vielen Fällen daher dringend auf den Prüfstand, zumal sich heute abzeichne, dass das Arbeiten von zu Hause auch nach der Corona-Zeit eine Option für den Berufsalltag ist.
Ein Homeoffice-Arbeitsplatz sei nicht per se unsicher, aber stärker gefährdet. Warum? Der Laptop befinde sich nicht mehr im geschützten Unternehmens- oder Behördennetzwerk, in welchem die IT-Abteilung Sicherheitsrichtlinien durchsetzt. In den eigenen vier Wänden bilde der Arbeits- (oder Privat-)Rechner einen Teil des Heimnetzwerks. Über dieses sollte ein Mitarbeiter mit einem kryptografisch abgesicherte Virtual Private Network (VPN) eine Verbindung etwa in die firmeneigene Infrastruktur aufbauen, schreibt Geese. Zum einen vergrößere sich dadurch jedoch die Angriffsfläche, zum anderen steige die Wahrscheinlichkeit, dass Schwachstellen auftreten.

Support notwendig

Ein schlecht oder gar nicht gesichertes WLAN mache es Hackern leicht, mit Viren oder Trojanern anzugreifen. Mitarbeiter müssten deshalb das Standard-Administrator-Passwort für ihr WLAN zu Hause durch ein neues, starkes Passwort ersetzen. Ebenso grundlegend sei es, die WPA2-Verschlüsselung (Wi-Fi Protected Access 2) zu aktivieren. Bereits bei diesen Basics sollte die interne IT für etwaige Unterstützung parat stehen. Ihr Support sei zudem notwendig, um festzustellen, auf welchem Sicherheitsniveau sich das Heimnetzwerk und seine angeschlossenen Geräte bewegen. Fakt sei: Das schwächste Glied bestimmt über die Sicherheit im gesamten Netzwerk. Auch der Uralt-PC für die Kinder brauche das aktuelle Antivirus-Update, damit dieser keine Schad-Software im Unternehmens- oder Behördennetzwerk verbreitet. Weitere wichtige zu klärenden Fragen sind laut Geese unter anderem: Auf welchem Release-Stand ist der Router? Und trennen Mitarbeiter strikt Arbeits- und Privatnutzung?

Rollenbasierte Zugriffsrechte

Wie Mitarbeiter Daten austauschen und teilen, regeln Unternehmen und Behörden in rollenbasierten Zugriffsrechten. Diese müssten sie auf die Nutzergruppen im Homeoffice übertragen und anpassen. Technisch lasse sich der Zugriff auf benötigte Ressourcen via VPN realisieren. Allerdings hänge die Sicherheit davon ab, wie die virtuellen Sicherheitstunnel konfiguriert sind. So habe die Einstellung, bei der reine Internet-Anfragen vom Homeoffice aus direkt an einen Server im Internet gehen, eine mögliche Konsequenz: Einem Mitarbeiter wird das Nutzerrecht eingeräumt, Dateien aus dem Internet herunterzuladen und zu installieren. So bestehe die Gefahr, dass er seinen Laptop mit Schad-Software infiziert. Dieses Szenario lasse sich verhindern, indem der gesamte Datenverkehr über die Unternehmens

oder Behörden-IT gelenkt wird. In dem Fall würden Firewalls beim Download greifen.

An Schwachstellen-Management anbinden

Wichtiger Bestandteil eines Sicherheitskonzepts ist ein leistungsfähiges Schwachstellen-Management, erklärt der Greenbone-COO. Dieses sollte auch Homeoffice-Umgebungen kontinuierlich auf Sicherheitslücken scannen und Gegenmaßnahmen vorschlagen, wie Konfigurationsanpassungen und Patches. Bevor eine cloudbasierte Lösung wie die Greenbone Managed Service Platform (GMSP) Homeoffice-Netze schnell, einfach und zuverlässig auf Schwachstellen durchleuchte, müsse die interne IT lediglich ein neues Gateway auf der Cloud-Plattform anlegen und dem Mitarbeiter zur Verfügung stellen. Die Nutzer würden es dann als virtuelle Maschine etwa auf dem Firmen-Laptop installieren und den Scan starten.
Der Weg zum sicheren Heim- und damit Unternehmensnetzwerk führe über sicheres WLAN zu Hause, rollenbasierte Zugriffsrechte, richtig konfigurierte VPN ins Firmen- oder Behördennetz und ein Schwachstellen-Management, das ständig auch die Homeoffice-Umgebungen auf Gefahrenquellen scannt. Zusätzlich müssten Firmen und Behörden ihre Mitarbeiter sensibilisieren, sodass diese auch gewiefte Phishing-Versuche erkennen und entsprechend gegensteuern können.

(co)

Stichwörter: IT-Sicherheit, Greenbone, Homeoffice, Schwachstellen-Management, VPN