Wie das Home Office sicher wird

Das Interesse an Heimbüros steigt, und auch mobiles Arbeiten von unterwegs gewinnt an Bedeutung. Auf diese Mobilität müssen sich Unternehmen sicherheitstechnisch einstellen.

Von Martin Setzler, Serviceleiter der AEB GmbH in Stuttgart

Mobile Working lässt sich auf vier Weisen umsetzen, die unterschiedliche Risiken mit sich bringen:

1. Vollständig von der Firma losgelöstes Arbeiten: Der Mobile Worker nimmt seine relevanten Daten mit. Diese müssen über ein sicheres Medium transportiert werden (auf verschlüsselten Festplatten, USB-Sticks oder direkt auf dem mobilen Arbeitsgerät). Hier kann es neben den Sicherheitsbedenken und den vielen Fehlermöglichkeiten durch unachtsamen Umgang mit den Medien und Daten auch Probleme mit asynchronen Dateien geben.

2. Anbindung nur an bestimmte firmeninterne Systeme: Der Mitarbeiter erhält nur Zugriff auf Mail und Kalender über Mechanismen wie Microsoft Exchange Web Services. Alternativ können ihm auch Teile des Intranets als passwortgeschütztes Extranet zur Verfügung gestellt werden. Neben unverschlüsselten Kommunikationsverbindungen über ungeschützte WLAN-Strecken ist ein weiteres Problem, dass von außerhalb leicht auf Daten zugegriffen werden kann. Selbst die von außen verfügbaren Systeme in separate Sicherheitszonen wie DMZ auszulagern, hilft nur bedingt.

3. Arbeiten in der Public Cloud: Hier geht es etwa um ein CRM-System, das in der Cloud liegt oder um Dokumente auf Cloud-Plattformen wie Sharepoint (OneDrive) oder Dropbox. Die Problematik mit dem Zugriff von außen auf interne Systeme besteht hier nicht. Allerdings sollten besonders deutsche Unternehmen bei dieser Variante genau hinsehen. Sobald personenbezogene Daten betroffen sind, verstößt man schnell gegen das Bundesdatenschutzgesetz. Auch der Abschluss eines Auftragsdatenverarbeitungsvertrags mit dem Cloud-Anbieter hilft nur, wenn sichergestellt ist, dass die Daten nicht ins außereuropäische Ausland gelangen können. Das ist bei vielen bekannten Cloud-Anbietern der Fall. Ganz zu schweigen von den Möglichkeiten amerikanischer Behörden, die aufgrund des Patriot Act bei amerikanischen Cloud-Anbietern uneingeschränkte Einsicht in die Daten bekommen.

4. Zugriff per VPN/Remote Desktop: Hier geht es um transparentes Arbeiten im Firmennetz über Virtual Private Networks (VPN) oder Remote-Desktop-Varianten (Citrix-Lösungen, Microsoft Terminal Server und ähnliche Techniken). Die Arbeit erfolgt nach dem Login über ein Gateway. Hier bestehen wieder die Risiken, die ein direkter Zugriff auf Ressourcen des Firmennetzes birgt, auch wenn dabei die Kommunikation wenigstens gesichert (weil verschlüsselt) abläuft.

Eine große Sicherheitslücke in allen vier Fällen stellen das Endgerät des Anwenders und die Netzstrecke dar. Kann die IT bei firmeninternen Geräten bestimmte Sicherheitsmindestanforderungen auch technisch durchsetzen und erfüllen, so fällt das bei den vorgestellten Mobile-Working-Varianten schwer. Dieser Schutz des Endgeräts (Device Protection) ist nur teil-

weise möglich. Zwar gibt es verschiedene Ansätze, um die Risiken in den Griff zu bekommen. Dazu zählen etwa gerätespezifische Policies, die dafür sorgen, dass wenigstens die wichtigsten Sicherheitskomponenten auf den Clients installiert und aktiviert sind – etwa automatische Sperre, Entsperren nur durch Passwort, Malware-Scanner und Firewalls. Zudem helfen Outer-Perimeter-Defence-Maßnahmen wie Network-Access-Control-Mechanismen. Mit diesen haben nur zugelassene Geräte Zugriff auf das Firmennetz, und es kann sichergestellt werden, dass die sicherheitsrelevanten Komponenten aktiv sind. Auch Unified-Thread-Management-Lösungen oder Next-Generation-Firewall-Strukturen in Kombination mit anderen Techniken können die Sicherheit weiter erhöhen. Allerdings sind diese Techniken relativ teuer und müssen intensiv betreut werden. Zudem lassen sich damit nur bekannte Geräte oder Geräte, auf denen Zertifikate eingespielt wurden, sinnvoll absichern. Andere Devices bleiben außen vor.

Eine weitere Schwachstelle ist der Mensch. Beim Thema Informationssicherheit rangiert seit Jahren menschliches Verhalten unter den Gefahrenquellen ganz oben. Der Mensch stellt auch deshalb solch ein großes Risiko dar, weil Zugänge immer noch viel zu häufig nur über ein Benutzerkonto und ein Passwort gesichert sind. Das ist nicht nur deswegen unzureichend, weil Mitarbeiter dazu tendieren, sorglos oder unsicher mit ihren Passwörtern umzugehen. Das Problem ist auch, dass trotz (oder gerade wegen) aller Komplexitätsregeln für Passwörter heute häufig Passwörter geknackt werden. Auch gibt es noch immer Menschen, die Passwörter notieren und in die Laptop-Tasche stecken oder unter die Tastatur schreiben. Ein weiterer klassischer Fehler: Der Anwender verwendet ein und dasselbe Passwort für mehrere Konten. Auch als Folge solchen Verhaltens treten immer wieder Sicherheitslücken in großen Unternehmen auf, durch die Hunderttausende Passwörter in die falschen Hände geraten.

Abhilfe schafft nur eine Zwei-Wege-Authentifizierung mit einem Einmalkennwort (One Time Passwort = OTP). Neben dem Passwort hat der Benutzer hier eine zweite Geheiminformation, die nur für wenige Sekunden gültig ist. Diese wird losgelöst vom Login-Vorgang idealerweise auf einem anderen Gerät generiert oder bereitgestellt, etwa per SMS auf dem Smartphone.

Trotz aller Unwägbarkeiten ist sicheres Mobile Office möglich. Zwei-Wege-Authentifizierung reicht aber nicht aus, um die Sicherheitslücken zu schließen, die das menschliche Verhalten reißt. Unternehmen sollten ein Informations-Sicherheits-Management-System (ISMS) installieren. Sie sollten sich hierbei an Best Practices wie den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) oder der Sicherheitsnorm ISO 27001 orientieren. Das hilft, das Thema Informationssicherheit zu strukturieren und über alle Ebenen zu betrachten sowie einen nachhaltigen Regelkreis zum Planen, Etablieren, Prüfen und Handeln zu etablieren (Plan – do – check– act, PDCA-Zyklus). Das System sollte verbindlich festlegen, wie Mitarbeiter regelmäßig über Sicherheitsthemen informiert und darin geschult werden und wie die Wirksamkeit der Schulungen gemessen wird. Kontinuierliches Prüfen, Messen und Verbessern muss auch für Menschen und ihr Verhalten etabliert werden. Am wichtigsten ist dabei, die Aufmerksamkeit der Mitarbeiter zu erhöhen und ihr Verständnis für Risiken und für das Sicherheitsbedürfnis des Unternehmens zu wecken. Das kann spielerisch geschehen – etwa durch einen Life-Hack-Event. Alternativ können an die Mitarbeiter immer wieder Hinweise versandt werden, die auch im privaten Umfeld hilfreich sind. Wichtig ist, dies langfristig geplant und kontinuierlich zu betreiben.

Gutes Mobile Working kann nur im Zusammenspiel all der erwähnten Überlegungen funktionieren: Gewählt werden muss die für die Aufgabe und das Unternehmen passende Mobile-Working-Variante. *(sh)*

Mobile Office im täglichen Einsatz

Beim Stuttgarter IT-Dienstleister AEB GmbH nutzen etwas mehr als 60 Prozent der Mitarbeiter Mobile Office, entweder via Smartphone oder via Citrix:

1. Zugriff auf Postfächer und Kalender vom Smartphone aus. Neben dem Benutzernamen und dem Passwort dient das Gerät selbst als zweite Authentifizierung. Über die Geräte-ID und Zertifikate wird sichergestellt, dass nur berechtigte Mobile Devices Zugriff erhalten. Auf diesen werden alle relevanten Sicherheitseinstellungen durchgesetzt.

2. Zugriff zu allen firmenrelevanten Programmen auf einer zentralen Citrix-Farm via Citrix Access Gateway. Neben Benutzername und Passwort wird hier für den erfolgreichen Zugang ein Einmal-Passwort benötigt. Dies wird per mOTP-App erzeugt oder per SMS an den Mitarbeiter versandt. Auf der Citrix-Farm laufen alle firmenrelevanten Programme und werden den Mitarbeitern als Published Applications zur Verfügung gestellt. Je nach Rolle bekommen die Mitarbeiter die für sie notwendigen Anwendungen. Mitarbeitern mit besonderen Anforderungen an Software und Rechnerressourcen, etwa für Programmieraufgaben, steht ein Rechner im firmeneigenen Rechenzentrum (Blade-PC) zur Verfügung. Auf diesen können sie über das Citrix Access Gateway zugreifen.

3. Eine Security Policy ist verabschiedet und allen Mitarbeitern bekannt. Durch regelmäßige Security-Awareness-Maßnahmen wird auf Gefahren und Risiken ebenso hingewiesen und das allgemeine Sicherheitsverständnis geschärft.