INFOPAPER:
SO GELINGT IT-SICHERHEIT IM HOME OFFICE

Inhalt

Einleitung

Der Wecker klingelt später, man kann zu Hause Mittag essen und die Kinderbetreuung lässt sich auch einfacher regeln. Arbeiten im Home Office kann viele Vorteile haben. Dabei sollten jedoch einige Punkte nicht außer Acht gelassen werden, damit auch außerhalb des Unternehmens die IT-Sicherheit gewährleistet wird. Hornetsecurity hat dafür einige Empfehlungen parat.

Home Office - aber nur mit den richtigen Sicherheitsvorkehrungen

Das Fortschreiten der Digitalisierung und die Entwicklung neuer Technologien brachten bereits viele Veränderungen für die Wirtschaft weltweit mit sich: Cloud-Computing, Big-Data, Robotik und Künstliche Intelligenz bieten Unternehmen bereichs- und branchenübergreifend Vorteile, wie beispielsweise die Optimierung von Prozessen, Einsparungen von Ressourcen und einen raschen Daten- und Informationsaustausch. Neue Unternehmen und Arbeitsplätze entstehen auf Basis dieser Entwicklungen.

Zudem führte der Trend zu **Veränderungen in der Arbeitswelt:** Viele Arbeitnehmer können standortunabhängig ihren Aufgaben nachkommen und dennoch weiterhin mit ihren Kollegen und dem Arbeitgeber kommunizieren. Unternehmen machen es ihren Mitarbeitern so möglich auch von zu Hause aus arbeiten zu können.

Als großer Treiber der kollaborativen Arbeit über die Cloud gilt **Microsoft Office 365**. Wichtige Dateien können von überall in Echtzeit gespeichert und ausgetauscht werden. Das vereinfacht die Arbeit im Home Office zusätzlich. In besonderen Krisenzeiten, wie wir es alle mit der Coronavirus-Pandemie erlebt haben, ist Home Office für Unternehmen sogar oftmals die einzige Möglichkeit für die Sicherheit ihrer Mitarbeiter zu sorgen und gleichzeitig den Geschäftsbetrieb aufrecht zu erhalten.

Sowohl bei Arbeitgebern als auch Arbeitnehmern kommen jedoch **immer wieder Fragen zum Thema IT-Sicherheit** auf:

- Wie kann der Schutz der unternehmensweiten IT-Infrastruktur auch vom Heimarbeitsplatz aus gewährleistet werden?
- Müssen Unternehmen und Mitarbeiter bestimmte Maßnahmen ergreifen?
- Sind Schutzmechanismen wie Spam- und Virenfilter auch im Home Office aktiv?

Im Folgenden klären wir über die Risiken im Home Office auf und erläutern mögliche Sicherheitsvorkehrungen, die zu beachten sind, um auch von zu Hause aus den **Schutz der unternehmensinternen Daten und der Kommunikation sicherzustellen.**

Schulen Sie Ihre Mitarbeiter und klären Sie über potenzielle Gefahren auf

Zuallererst ist zu beachten: Mitarbeiter sollten **über mögliche Sicherheitsrisiken und zu treffende Schutzmaßnahmen aufgeklärt werden**, bevor es ins Home Office geht.

Geben Sie deutliche, unmissverständliche und **verbindliche Regelungen zur IT-Sicherheit** und zur Sicherheit der Unternehmensdaten in schriftlicher Form vor, damit das Vorgehen transparent für alle nachvollziehbar ist.

Dabei ist es insbesondere wichtig nicht nur über Vorkehrungen zu informieren, sondern auch für **potenzielle Gefahren** wie beispielsweise Phishing-Attacken zu sensibilisieren, die selbstverständlich auch vor der Arbeit im Home Office nicht halt machen.

Stellen Sie außerdem sicher, an wen sich Mitarbeiter wenden können, sollten sicherheitsrelevante Probleme auftauchen, um eine schnelle Reaktion zu ermöglichen.

Sichern Sie Ihre Unternehmensdaten und nutzen Sie VPN-Clients

Das WLAN zu Hause, im Café oder im Zug kann Sicherheitsrisiken bergen. Wenn Arbeitnehmer über ein solch ungesichertes Netzwerk auf **sensible Daten** zugreifen oder sich in Geschäftskonten einloggen, besteht für das Unternehmen bei einem Hackerangriff die Gefahr, dass Cyberkriminelle Informationen abgreifen.

Unternehmen müssen daher Sicherheitsmaßnahmen etablieren wie beispielsweise **Virtual-Private-Network-Lösungen (VPN)** für den Einsatz im Zusammenspiel mit WLAN.

Der VPN-Dienst kann zusätzlich noch um eine 2-Faktor-Authentifizierung ergänzt werden und beim Arbeiten über VPN sollte der Arbeitgeber darauf achten, Zugriffsrechte zu beschränken, sodass jede Person nur auf die für sie relevanten Informationen zugreifen kann.

Zugleich besteht auch das Risiko eines Datenverlustes, wenn ein Mitarbeiter sensible Informationen auf einem Laptop speichert, der im schlimmsten Fall dann gestohlen wird.

Sensible Daten sollten daher im besten Fall lediglich **auf sicheren Unternehmensservern oder in Cloud-Umgebungen gespeichert** werden, die nur mittels VPN aufgerufen werden dürfen. Sollten Daten dennoch auf externe Festplatten gespeichert werden, gilt es, diese Informationen oder den Zugang zu verschlüsseln.

Verhindern Sie die Einsicht und den Zugriff von Unbefugten

Zur effektiven Nutzung von Reisezeiten wird auch viel **von unterwegs gearbeitet**, beispielsweise am Flughafen oder im Zug.

Das Problem dabei ist allerdings, dass Sitznachbarn die Möglichkeit bekommen, Firmeninterna zu lesen.

Blickschutzfilter sollten deshalb eine Selbstverständlichkeit darstellen, sobald außerhalb des Büros der Zugriff auf sensible Firmendaten erfolgt. Zusätzlich muss unmittelbar eine **Bildschirmsperre** aktiviert werden, **sobald der Mitarbeiter sich vom Rechner entfernt** – diese Maßnahme sollte auch in den heimischen vier Wänden befolgt werden.

Selbstverständlich muss der Zugriff auf den Rechner beim Starten **durch ein Passwort freigeschaltet** werden.

Stellen Sie unternehmenseigene Hardware zur Verfügung

Eine große Sicherheitslücke stellt das Endgerät des Anwenders dar.

Während die Unternehmens-IT noch verhältnismäßig einfach bei firmeneigenen Geräten bestimmte Sicherheitsmindestanforderungen auch durchsetzen und sicherstellen kann, so fällt dies bei Privatgeräten der Mitarbeiter schwer.

Der Schutz dieser Endgeräte ist nur teilweise möglich. Insbesondere USB-Sticks und externe Festplatten gelten als **Einfallstor für Schadsoftware**. Es gibt allerdings verschiedene Ansätze, um die Risiken in den Griff zu bekommen. Dazu zählen etwa **gerätspezifische Policies**, die sicherstellen, dass wenigstens die wichtigsten Sicherheitskomponenten auf den Clients installiert und aktiviert sind - beispielsweise automatische Sperre, Entsperren nur durch Passwort oder Malware-Scanner und Firewalls.

Zudem helfen Maßnahmen wie **Network-Access-Control (NAC)-Mechanismen.** Mit diesen haben nur zugelassene Geräte Zugriff auf das Firmennetz und es kann garantiert werden, dass die relevanten Komponenten aktiv sind. **Am sichersten ist jedoch die Verwendung der unternehmenseigenen Hardware.**

Installieren Sie aktuelle Sicherheitssoftware

Alle Unternehmensgeräte, inklusive Smartphones und Laptops, sollten durch geeignete und **aktuelle Sicherheitssoftware** geschützt werden. Diese umfassen bestenfalls **Funktionen zur Datenlöschung von Geräten**, die als verloren oder gestohlen gemeldet werden, die Trennung von persönlichen und beruflichen Daten sowie die Einschränkung der Installationsmöglichkeiten von Apps.

Doch nicht nur Geräte müssen mit Sicherheitssoftware abgesichert werden, **auch Anwendungen und Dienste** geraten ins Visier von Cyberkriminellen. Eines der beliebtesten Angriffsziele: **Microsoft Office 365**. Rund 180 Millionen Unternehmenskunden verzeichnet der internationale Technologiekonzern Microsoft derzeit bei seinem Dienst. Da Office 365 cloudbasiert ist, eignet es sich natürlich **ideal für die Arbeit im Home Office**.

Einen Office 365-User zu identifizieren, ist für einen Angreifer allerdings sehr simpel, denn die MX-Records und Autodiscover-Einträge sind im Netz öffentlich einsehbar. **Umfassende Security-Features** sollen mögliche Angriffe von Office 365-Accounts abwehren, doch muss bedacht werden, dass die Daten in der Cloud selbst – auch bei einem unbefugten Zugriff – von überall abrufbar sind. Durch die Nutzung von Office 365 entfällt den Unternehmen ein wichtiger Sicherheitsaspekt: die Firewall.

Gelingt es einem Angreifer unbefugt Zugriff zu einem Office 365-Account zu erlangen, stehen ihm alle Daten uneingeschränkt zur Verfügung. Security-Experten empfehlen daher sich nicht allein auf die Schutzmechanismen von Microsoft zu verlassen, sondern Office 365-Accounts zusätzlich **durch Drittanbieter-Lösungen abzusichern.**

Spezialisierte Anbieter verbergen beispielsweise die Microsoft-DNS- und MX-Records, wodurch Office 365-Nutzer für die Angreifer nicht einfach identifizierbar sind und allein dadurch seltener ins Visier geraten.

Schützen Sie sich vor dem Ausfall der E-Mail-Kommunikation

Per E-Mail-Nachricht werden Verträge, wichtige Informationen sowie Kontaktdaten ausgetauscht.

Sollte allerdings der unternehmenseigene E-Mail-Server über einen längeren Zeitraum hinweg ausfallen, ist dies vor allem für Mitarbeiter im Home Office fatal.

Der Support ist nicht wie gewohnt schnell zur Stelle und den Unternehmen drohen durch den längerfristigen **Kommunikationsausfall** Komplikationen im Geschäftsbetrieb.

Wichtig ist gerade dann, dass es Alternativ-Lösungen gibt, die im Notfall einspringen, so dass keine E-Mails verloren gehen und Nachrichten weiterhin versendet und empfangen werden können.

Ein **Continuity Service ist hier die Lösung**. Dabei erkennt ein autarkes Monitoring, wenn der Mailserver des Kunden ausgefallen ist. Der Continuity Service wird in einem solchen Fall **automatisch und unmittelbar aktiviert.**

Die Zustellung der E-Mails erfolgt ohne Unterbrechung auf alternativem Wege (POP3/IMAP-Postfach oder Webmail-Zugang). Der Zugriff auf gesicherte E-Mails bleibt somit auch während des Ausfalls beispielsweise direkt aus Outlook heraus erhalten.

Checkliste

Mit der folgenden Checkliste von Hornetsecurity haben Sie eine Übersicht der wichtigsten Punkte, die für die **IT-Sicherheit im Home Office** zu beachten sind:

- ☑ **Mitarbeiterschulungen helfen, um über potenzielle Gefahren aufzuklären**
- ☑ **VPN-Clients sorgen für eine sicheren Zugriff auf sensible Daten im Unternehmensnetzwerk**
- ☑ **Die Einsicht und der Zugriff von Unbefugten auf die Arbeitsgeräte muss vermieden werden**
- ☑ **Unternehmenseigene Hardware minimiert Sicherheitsrisiken**
- ☑ **Aktuelle Sicherheitssoftware und zusätzliche Drittanbieter-Lösungen für Office 365**
- ☑ **Continuity Services verhindern im Ernstfall den Ausfall der E-Mail-Kommunikation**