#WIRtuell im Homeoffice – aber sicher!

12 Tipps, damit Ihre MitarbeiterInnen remote reibungslos arbeiten können.

1 Sicheren Internet- und Intranetzugriff verwenden

Aufgrund der massiv gestiegenen Anzahl an Homeoffice-UserInnen kommt es zu einer hohen Auslastung der Netzwerke. So stossen Firewalls oder auch VPN-Konzentratoren schnell an ihre Grenzen. Vielfach sind VPN-Lösungen deshalb so konfiguriert, dass ein Teil der Zugriffe direkt in das Internet abgeführt werden und nur der Datenzugriff, der in Richtung Unternehmensnetzwerk geht, über das VPN geführt wird. Das führt jedoch dazu, dass unternehmensinterne Sicherheitsmechanismen wie Intrusion Detection Systeme oder auch Sicherheitsfilter auf Proxy-Servern nicht mehr greifen. Über eine kompromittierte Website können daher Angriffe direkt auf das MitarbeiterInnen-Notebook gelangen und so auch potentiell Angreifern Zugriff auf das Unternehmensnetzwerk ermöglichen. Um dies zu verhindern, sollte der gesamte Netzwerkverkehr über die VPN-Verbindung und die zentralen Sicherheitssysteme des Unternehmensnetzwerkes geführt werden oder alternativ eine Cloud Security Lösung genutzt werden. Diese bewirken, dass Zugriffe ins Internet direkt erfolgen, jedoch trotzdem alle Sicherheitsmechanismen greifen.

2 Im Homeoffice auf Daten zugreifen und zusammenarbeiten

Collaboration Tools sind in einer modernen IT unverzichtbare Werkzeuge, umso mehr für MitarbeiterInnen die im Homeoffice arbeiten müssen. Zur Mindestausstattung zählen eine aus dem Homeoffice erreichbare Datenablage- sowie Austauschplattform, eine Video- oder Telefonkonferenzlösung, sowie eine Chatplattform, die eine sichere Kommunikation im Unternehmen auch remote ermöglicht. Nicht vergessen werden sollte, dass auch im Homeoffice Dokumente unterschrieben werden müssen. Die Einrichtung einer elektronischen Signaturlösung stellt somit eine sinnvolle Massnahme dar.

3 Zugangsdaten (Credentials) absichern

Gerade bei Arbeiten im Homeoffice sind die Zugangsdaten gegen Missbrauch und Entwendung möglichst gut abzusichern. Besonders bei MitarbeiterInnen, die mit hohen Rechten auf unternehmenskritische IT-Systeme zugreifen, wie beispielsweise IT-Techniker, ist eine Verifizierung durch eine Zwei-Faktor-Authentifizierung empfehlenswert.

4 Lösungen zur Absicherung von Endgeräten einsetzen

Notebooks sind ausserhalb des Unternehmensnetzwerks – so auch im Homeoffice – nicht durch die Infrastruktur des Unternehmensnetzwerks geschützt. Firewalls und Intrusion Detection Systeme sind nur für Zugriffe über VPN wirksam und die Erkennung bzw. Reaktion auf Anomalien ist ohne geeignete Lösungen schwierig. Umso wichtiger ist deshalb der Einsatz einer modernen Endpoint Detection & Response (EDR) Lösung. Diese ermöglicht eine Untersuchung aller Prozesse und Applikationen am Endgerät auf Anomalien. Im Falle eines Angriffs oder dem Zugriff auf eine infizierte Website können rasch Gegenmassnahmen ergriffen werden. So kann bspw. die Installation einer Malware unterbunden oder im Bedarfsfall das Gerät unter Quarantäne gesetzt werden, um bspw. den Ausbruch eines Crypto-Trojaners oder auch den Zugriff eines Angreifers auf Unternehmensdaten zu verhindern.

5 Device-Hardening-Konzept umsetzen

Gerade im Homeoffice ist eine Absicherung des Endgeräts durch eine korrekte Konfiguration der Einstellungen – idealerweise auf Basis eines aktuellen Device-Hardening-Konzepts – von grosser Bedeutung. Wird dies vernachlässigt, können grundlegende Sicherheitsfunktionen nicht mehr greifen, unberechtigte Zugriffe via Fernwartungszugänge werden möglich oder Netzwerkfreigaben für Dritte zugänglich. Ein umfassenden Hardening-Konzept beinhaltet die Deaktivierung nicht benötigter Dienste, die Deinstallation nicht erforderlicher Software, die Anpassung von Zugriffsrechten, die Verschlüsselung lokaler und mobiler Datenträger sowie eine eingeschränkte Verwendung hochprivilegierter Benutzerkennungen. Genau solche hochprivilegierte Kennungen sollten generell nur mit einer 2-Faktor-Authentifizierung verwendet werden.

6 Laufendes Patchmanagement sicherstellen

Unter regulären Arbeitsbedingungen werden Updates gegen Sicherheitslücken dann installiert, wenn sich die Geräte im Unternehmensnetzwerk befinden und hohe Datendurchsatzraten genutzt werden können. Sind die Devices nun für einen längeren Zeitraum im Homeoffice platziert, muss das Client-Patchmanagement entsprechend angepasst werden, sodass auch weiterhin das regelmässige Einspielen von Sicherheitsupdates trotz eingeschränkter Durchsatzraten zu den zentralen Softwareverteilungsstellen gewährleistet wird.

7 Home-Network-Security verbessern

Im Homeoffice kann das private Netzwerk der MitarbeiterInnen Sicherheitslücken, wie veraltete bzw. kompromittierte Router/Modems oder schwache WLAN-Passwörter, bergen. Die MitarbeiterInnen müssen auf diese Risiken aufmerksam gemacht und aufgefordert werden, Router ggf. zu tauschen und den Unternehmensrichtlinien entsprechende Passwörter einzustellen.

8 MitarbeiterInnen vermehrt über Cybercrime aufklären

MitarbeiterInnen sind häufig Ziel von Phishing Mails und Social Engineering Attacken – besonders in Zeiten erhöhter Unsicherheit. Eine laufende Sensibilisierung der UserInnen zum Umgang mit bspw. unglaubwürdigen E-Mail-Adressaten oder Webseiten ist unbedingt notwendig. Die Meldung solcher Cybercrime-Versuche an die Security-Verantwortlichen ist wichtig. So können zeitnah Aufklärungsinformationen an die gesamte Belegschaft ausgeschickt und entsprechende technische Massnahmen ergriffen werden, um etwaige Angriffe abzublocken.

9 Sicherheit und Funktionalität gewährleisten

Bei Performance Problemen oder fehlenden Zugriffsmöglichkeiten auf Unternehmensapplikationen passiert es häufig, dass einzelne MitarbeiterInnen unüberlegt eigenmächtig Umgehungslösungen nutzen. Nicht selten werden Applikationen mit sensiblen Informationen dadurch für Zugriffe ins Internet freigeschaltet und ermöglichen somit unberechtigten Dritten potentiell Zugriff auf sensible Unternehmensdaten, da sie weder zentral verwaltet noch korrekt abgesichert sind. IT Security muss als ganzheitliches Konzept erstellt und auch umgesetzt werden, sodass die IT Abteilung diese Entwicklungen rechtzeitig erkennen und gegensteuern kann.

10 Richtigen Umgang mit Unternehmensdokumenten kommunizieren

Werden beim Arbeiten im Homeoffice Geschäftsdokumente ausgedruckt und ist über einen längeren Zeitraum der Zutritt zu den Geschäftsräumen mit sicheren Entsorgungsmöglichkeiten ausgeschlossen, dann steigt das Risiko, dass solche Dokumente aus Versehen oder Nachlässigkeit im Hausmüll landen. Ausserdem können kritische oder sogar unter Geheimhaltung fallende Dokumente vermehrt vom Büro nach Hause genommen werden. Dadurch steigt die Wahrscheinlichkeit, dass Nicht-Firmenangehörige Zugang zu diesen bekommen. Grundsätzlich gilt es alle MitarbeiterInnen zu informieren: So wenig wie möglich auszudrucken, einen sorgsamen Umgang mit Dokumenten zu pflegen und nicht vermeidbare Ausdrucke im Büro entsprechend zu vernichten.

11 Business Continuity Pläne überarbeiten

Oft ist die IT- und Netzwerkarchitektur nur für den Alltagsbetrieb ausgelegt. Eine drastisch erhöhte Anzahl von Zugriffen von ausserhalb des Firmennetzwerks über einen längeren Zeitraum ist nicht vorgesehen. Das IT Service Continuity Management (ITSCM) muss diese Situation neu evaluieren, eventuelle Bottlenecks sowie Single Point of Failure identifizieren und entsprechende Anpassungen vornehmen, um die Business Continuity auch für solche Rahmenbedingungen zu gewährleisten.

12 DDoS-Früherkennung implementieren

Durch die erhöhte Anzahl der Homeoffice-UserInnen und dem daraus resultierendem Anstieg des Netzwerk-Traffics stossen viele Systeme an ihre Kapazitätsgrenzen. Dadurch steigt auch das Risiko von DDoS-Attacken erheblich an. Mit DDoS-Früherkennungs-Massnahmen können diese Attacken rechtzeitig erkannt und mit entsprechenden technischen Einrichtungen gegengesteuert werden.

Bei Fragen steht Ihnen unser Experte gerne zur Verfügung:
Freddy Bürkli
+41 792 614549
freddy.buerkli@t-systems.com
www.t-systems.ch

T · · Systems ·
Let's power higher performance

Herausgeber: T-Systems Schweiz AG | Industriestrasse 21 | 3052 Zollikofen | Version 03/2020