WHITEPAPER

So sichern Sie Netzwerke mobiler Mitarbeiter

GFI™

Aurea SMB Solutions

Inhaltsverzeichnis

Einleitung

Ihr kleines Unternehmen hat sich auf eine Weise verändert, die Sie nie erwartet hätten. Auch wenn Ihr Unternehmen den gesamten Geschäftsverkehr nicht nur im Homeoffice abwickelt, möchten Sie, dass die Netzwerke Ihrer Mitarbeiter sicher sind. Infolgedessen hat sich Ihr Unternehmen möglicherweise teilweise oder vollständig online verlagert.

Dies erschwert die Notwendigkeit, alle Dateien und die gesamte Kommunikation sicher zu verwahren. Die Geräte, mit denen Ihr Unternehmen arbeitet, befinden sich möglicherweise nicht mehr nur in Ihrem Büro.

Was ist also zu tun? Ihr Budget ist knapp bemessen. Sie haben keine IT-Experten in Ihrem Team für mobile Mitarbeiter. Ihr Geschäftsplan war wahrscheinlich nicht darauf vorbereitet, die Sicherheit bei Eintreten eines Katastrophenfalls zu gewährleisten, bei dem alle Mitarbeiter im Homeoffice arbeiten müssen.

Viele Unternehmen haben bereits vor der COVID-19-Pandemie mit dem Wechsel zu mobilen Mitarbeitern begonnen. Für die anderen bedeutet dies, dass es etablierte Konzepte und kosteneffiziente Softwares gibt, die Ihnen das Leben erleichtern und Ihr Unternehmen schützen.

Sicherheitsprobleme, die IT-Administratoren berücksichtigen müssen, wenn es um mobile Mitarbeiter geht

Deutlich verbesserte Online-Kommunikation

Da so viel Interaktion und Kommunikation auf online umgestellt wurde, müssen Sie sicherstellen, dass Sie über eine solide E-Mail- und Kommunikationssicherheit verfügen.

Während die Sicherheit beim Video-Chat im Allgemeinen darauf hinausläuft, die datenschutzfreundlichste Software für Ihre Anforderungen auszuwählen, sind die Auswahlmöglichkeiten für E-Mails differenzierter. E-Mails müssen vor zahlreichen Bedrohungen geschützt werden, einschließlich unbefugtem Zugriff oder Verlust.

E-Mail-Angriffe können aus Phishing-Angriffen, Spam oder Malware bestehen, mit irreführenden Betreffen, Inhalten, Anhängen oder Links, die Benutzer dazu verleiten, diese zu öffnen. Sie benötigen einen umfassenden Anti-Spam-Service sowie eine Schulung der Mitarbeiter über Art und Erscheinungsbild dieser Angriffe.

Gezielte Phishing-Angriffe auf Mitarbeiter im Homeoffice werden wahrscheinlich zunehmen, da böswillige Unbefugte wissen, dass immer mehr Menschen in dieser neuen und möglicherweise weniger geschützten Umgebung arbeiten werden.

Es gibt zahlreiche Angriffe im Homeoffice und andere Angriffsmöglichkeiten, die Kosten verursachen, wichtige Informationen Gefahren aussetzen und Ihr Unternehmen für andere Angriffe verwundbar machen. Mögliche Hacking-Versuche können erkannt werden, wenn man weiß, wonach man suchen muss. Bieten Sie Mitarbeitern einen Auffrischungskurs an, um sie auf aktuelle E-Mail-Betrügereien und Phishing-Angriffe aufmerksam zu machen.

Böswillige Unbefugte verwenden möglicherweise weiterhin ungesicherte E-Mails als Zugangspunkt, um in Ihr Netzwerk zu gelangen. Um dies zu verhindern, stellen Sie sicher, dass jeder ein sicheres Kennwort hat und eine MFA (Multi-Faktor-Authentifizierung) aktiviert ist.

Als bewährte Methode sollte Ihr Unternehmen auch eine automatisierte E-Mail-Verschlüsselungslösung in Betracht ziehen, die den ausgehenden E-Mail-Verkehr analysiert, um sensibles Material zu erkennen und solche als sensibel eingestuften E-Mails zu verschlüsseln.

Wenn Sie einen großen, browserbasierten E-Mail-Client wie Google Mail verwenden, verschlüsseln Sie bereits jede E-Mail mit TLS (Transport Layer Security). Diese Art der Verschlüsselung ist nicht so sicher wie die End-to-End-Verschlüsselung, daher sollten Sie einen zusätzlichen Service für sensible Daten in Anspruch nehmen. Solange jeder in Ihrem Unternehmen die oben aufgeführten Ratschläge befolgt, um seine Konten zu schützen, Malware-Links zu vermeiden und Phishing-Schemata zu erkennen, sollte Ihre Kommunikation für mobile Mitarbeiter sicher sein.

Tools, die Sie für dieses Sicherheitsproblem benötigen

- Antivirenprogramm mit integriertem E-Mail-Scan
- Pishing-Tools und Internetsicherheitstools (normalerweise in Ihren Browser integriert)

Empfohlene Vorgehensweise

- Informieren Sie Ihre Mitarbeiter über alle gängigen Phishing- und Spam-Angriffe
- Achten Sie besonders auf alle Links und Anhänge, die per E-Mail gesendet werden, insbesondere von unbekannten Absendern
- Fordern Sie entsprechende Passwortbestimmungen
- Fordern Sie eine Zwei-Faktor-Authentifizierung
- Verwenden Sie sicherere, durchgängig verschlüsselte Methoden zum Senden vertraulicher Daten

Geräte mobiler Mitarbeiter scannen und patchen

Unter normalen Umständen befolgt Ihr IT-Team einen Zeitplan und eine Vorgehensweise, gibt wichtige Patches sofort heraus und befolgt Zeitpläne, um nicht lebenswichtige Patches über Nacht oder außerhalb der Arbeitszeit zu integrieren, um Ihre Mitarbeitern nicht bei der Arbeit zu stören. Jetzt arbeitet Ihr Netzwerk nicht mehr nur mit Computern in Büros.

Um die Sicherheit aller im Homeoffice zu gewährleisten, benötigen Sie eine Software, die alle Geräte Ihrer mobilen Mitarbeiter scannt und patcht. **Jeder dritte unbefugte Zugriff** wird durch nicht gepatchte Schwachstellen verursacht. Diese Sicherheitsverletzungen können verhindert werden, indem Sie einfach sicherstellen, dass Ihre Computer vollständig gepatcht sind.

Das ist zwar schwieriger mit Mitarbeitern im Homeoffice, aber nicht unmöglich. Es gibt Softwareoptionen, die genau für diesen Zweck entwickelt wurden. Ihr IT-Team kann seinen Sicherheitsplan mit geringfügigen Änderungen weiterhin befolgen. Die Geräte Ihrer Mitarbeiter bleiben auf dem neuesten Stand und darüber hinaus sicher, auch wenn sich diese im Homeoffice befinden.

Tools, die Sie für dieses Sicherheitsproblem benötigen

- Netzwerkmonitor
- Fernverwaltungssoftware

Empfohlene Vorgehensweise

- Bewerten Sie Ihr Netzwerk und erstellen Sie eine vollständige Inventarliste. Scannen Sie Ihr Netzwerk regelmäßig nach fehlenden Patches
- Stellen Sie sicher, dass alle Betriebssysteme in Ihrem Netzwerk abgedeckt sind (etwas, über das Sie sich wahrscheinlich keine Sorgen machen mussten, als noch nicht im Homeoffice gearbeitet wurde, weil in Ihrem Büro z. B. nur mit Windows gearbeitet wurde).
- Planen Sie Zeit für das Versenden von Patches ein, während Sie weiterhin auf wichtige Updates achten, die sofort übertragen werden müssen
- Führen Sie nach der Bereitstellung Tests aus und bereiten Sie sich darauf vor, Patches, die Probleme verursachen, zurückzusetzen, bis eine Lösung gefunden oder ein neuer Patch veröffentlicht wird
- Identifizieren Sie alle Sicherheitslücken mit regelmäßigen Scans, auch solche, die nicht auf fehlende Patches zurückzuführen sind

Sicherheit im Heimnetzwerk

Ein weiterer wichtiger Schritt zur Sicherung der Netzwerke mobiler Mitarbeiter besteht darin, sicherzustellen, dass das Sicherheitssystem ihres Heimnetzwerks funktioniert und stabil ist.

Verschlüsselung von Daten während der Übertragung

Wenn im Homeoffice gearbeitet wird, ist es wichtig, dass Ihre Mitarbeiter ihre Daten verschlüsseln. Um Materialien privat zu halten, sollte jeder in Ihrem Unternehmen zu Hause ein VPN verwenden, wenn auf vertrauliche Informationen zugegriffen wird.

Ein VPN liefert einen verschlüsselten Tunnel, der Ihren Datenverkehr schützt und Sie von Ihrer persönlichen IP-Adresse abbindet. Dies bietet Ihrem Unternehmen und Ihren Mitarbeitern mehr Privatsphäre.

Abhängig von dem VPN können Mitarbeiter durch Verbindungen zu potenziell ungesicherten Geräten ein höheres Risiko für das Netzwerk schaffen. Stellen Sie sicher, dass sich die Mitarbeiter dieses Risikos bewusst sind, und verwenden Sie das VPN nur, wenn Sie auf arbeitsbezogene Daten zugreifen.

Verschlüsseltes WLAN

Während es zwar selten vorkommt, dass auf ein persönliches WLAN zugegriffen wird, kann in diesem Fall ein Unbefugter alles abfangen, was Sie online senden oder eingeben: Bankinformationen, E-Mail-Konten, Zugangsdaten für Unternehmen und mehr.

Stellen Sie sicher, dass Ihr Netzwerk ordnungsgemäß konfiguriert ist und Sie Ihre Verbindung verschlüsseln. WPA2 oder jetzt WPA3 wird normalerweise als die beste Option für die WLAN-Verschlüsselung angesehen, und Ihr WLAN-Passwort muss sicher sein.

Änderungen am Router

Sie sollten Ihren Router-Login und Ihr Passwort ändern. Diese sind oft standardmäßig (z. B. ‘admin’) und sind schwach oder leicht zu erraten. Böswillige Unbefugte nutzen dies, um den Router zu erfassen, ihn in einen Bot zu verwandeln oder Angreifern zu ermöglichen, Sie auszuspionieren, während Ihre Online-Informationen über den Router gesendet werden. Stellen Sie sicher, dass Firmware-Updates automatisch installiert werden, um Sicherheitslücken zu schließen.

Abhängig von der Sicherheitsstufe, die Ihr Unternehmen benötigt, können Sie auch zusätzlichen Schritte unternehmen, mit denen die eingehenden und ausgehenden Transaktionen Ihrer Mitarbeiter eingeschränkt werden, Sie die höchste Verschlüsselungsstufe auswählen, die in ihren Router-Einstellungen möglich sind und Sie WPS ausschalten. Diese Schritte sind nicht benutzerfreundlich. Nutzen Sie dies also nur, wenn es unbedingt erforderlich ist.

Firewall-Anpassungen

Überprüfen Sie Ihre Firewall-Einstellungen mehrfach, um die Sicherheit Ihres Heimnetzwerks zu erhöhen. Firewalls bilden eine Barriere, um Bedrohungen zu verhindern, die versuchen, in Ihr System zu gelangen. Dies hilft auf zweierlei Arten: es verhindert, dass schädliche Programme in Ihr Netzwerk gelangen; und verhindert zudem, dass Daten von Ihren Heimgeräten nach außen gelangen.

In der Regel sind in Ihren Geräten bereits Firewalls integriert; stellen Sie sicher, dass diese in Ihren Einstellungen aktiviert sind. Kleine Unternehmen benötigen möglicherweise einen umfassenderen Sicherheitsplan durch externen Dienstleister, um die Firewall zu stärken.

Richten Sie Antivirenlösungen für persönliche Geräte ein

Während Geräte in Ihrem Büro möglicherweise bereits über einen Virenschutz verfügen, verwenden viele Mitarbeiter jetzt möglicherweise persönliche Geräte, die nicht über diesen verfügen. Selbst wenn sie die gegebenen Ratschläge befolgen, stellen schlecht gesicherte Geräte ein erhebliches Sicherheitsrisiko dar.

Stellen Sie sicher, dass die Computer, die Ihre Mitarbeiter zu Hause verwenden, leistungsstarke Antivirenlösungen enthalten. Dies umfasst unter Umständen den Kauf einer vertrauenswürdigen Antivirenlösung für die Geräte Ihrer Mitarbeiter, zumindest wenn diese über private Unternehmensinformationen verfügen müssen.

Es ist wichtig, dass Sie alle Informationen in Bezug auf Ihr Unternehmen schützen. Dazu gehören die Sicherung persönlicher Geräte und die Sicherstellung pünktlicher Aktualisierungen dieser Lösungen.

Tools, die Sie für dieses Sicherheitsproblem benötigen

- VPN
- Bandbreitenmanagement
- Erweiterte Firewall-Tools
- Antiviren-Lösung

Empfohlene Vorgehensweise

- Verwenden Sie immer ein VPN bei nicht vertrauenswürdigen Netzwerken
- Beachten Sie die Bandbreitenfunktionen des Remote-VPN eines Unternehmens
- Laden Sie das Remote-VPN Ihres Unternehmens nur auf Geräten herunter, mit denen Sie arbeiten
- Stellen Sie sicher, dass die VPN-Authentifizierungsmethode und die Verschlüsselung so gut wie möglich sind
- Überwachen Sie die eingehende und ausgehende Netzwerkkommunikation ständig auf verdächtige Aktivitäten
- Legen Sie ein sicheres Kennwort für Ihr drahtloses Netzwerk fest
- Verwenden Sie einen Router in Privatbesitz anstelle eines Routers, den Sie von Ihrem Internetdienstanbieter erhalten haben, und ändern Sie den werkseitigen Benutzernamen und das Kennwort
- Verwenden Sie die stärksten verfügbaren Firewall-Funktionen, mit denen Sie weiterhin wie gewünscht auf das Internet zugreifen können
- Implementieren Sie WPA2 oder WPA3 in Ihrem drahtlosen Netzwerk
- Halten Sie Ihren Router auf dem neuesten Stand
- Halten Sie Ihre Antivirenlösung auf dem neuesten Stand

Erstellen Sie ein Backup aller Daten mit einer verschlüsselten Sicherung

Daten werden ohne regelmäßige, verschlüsselte Backups nicht ordnungsgemäß gesichert. Dies gilt unabhängig davon, ob Ihre Mitarbeiter von zu Hause aus arbeiten oder nicht. Bei mobilen Mitarbeitern ist dies jedoch noch wichtiger.

Sie haben weniger Kontrolle über die Geräte von mobilen Mitarbeitern, daher können Sie nie ganz sicher sein, dass alle Geräte voll funktionsfähig und sicher sind. Sogar etwas so Einfaches wie das Verschütten von Kaffee über ein Gerät kann zu einem Datenverlust führen, wenn kein ordnungsgemäßer Backup erfolgt ist.

Ein gut gesichertes System stellt sicher, dass alle Unternehmensdaten verschlüsselt, hochgeladen und in einer zentralen Quelle gesichert werden können (häufig in einer Cloud, jedoch nicht zwingend), sodass Sie sich keine Sorgen machen müssen, aufgrund von menschlichem Versagen oder böswilligen Handlungen wichtige Daten zu verlieren.

Tools, die Sie für dieses Sicherheitsproblem benötigen

- Verschlüsselungsfähige Speichersoftware

Empfohlene Vorgehensweise

- Führen Sie Sicherungen häufig und regelmäßig durch
- Daten während der Speicherung verschlüsseln
- Entscheiden Sie, wie lange ein Backup erforderlich ist, abhängig von Ihrem Unternehmen und den Konformitätsbestimmungen
- Speichern Sie die wichtigsten Daten an mehreren Stellen (stellen Sie sicher, dass sie weiterhin verschlüsselt und ordnungsgemäß geschützt sind).

Wie schwierig ist es, Netzwerke mobiler Mitarbeiter zu sichern?

Viele dieser vorgeschlagenen Maßnahmen erfordern geringfügige Änderungen an Vorgehensweisen, die Sie bereits eingeführt haben oder durchgeführt haben, z. B. einen automatisierten Patch-Management-Service oder regelmäßige Sicherungen Ihrer Daten.

Einige Änderungen erfordern möglicherweise zunächst eine Anpassung, aber es gibt viele Produkte, die Unternehmen bei der Umstellung auf Mitarbeiter unterstützen, die vollständig oder teilweise im Homeoffice arbeiten. Wenn Sie einige einfache Vorgehensweisen befolgen und einige notwendige Tools hinzufügen, können Ihr Unternehmen und Ihre mobilen Mitarbeiter sicher arbeiten.

Schützen Sie Ihr Unternehmen mit dem Sicherheitslösungsset von GFI

Unlimited | Network Security

Vielschichtige Sicherheit zum Verhindern, Erkennen und Behandeln von Bedrohungen für Ihr Netzwerk

---

Secure Network with **Firewall & Intrusion Prevention**

Secure Traffic with **Web & Email Antivirus**

Secure Endpoints with **Vulnerability Monitoring & Patching**

Erfahren Sie mehr

GFI™

Aurea SMB Solutions