Vier einfache Möglichkeiten, Sessions am öffentlichen WLAN zu schützen

Sichere Verbindungen – überall und jederzeit – uneingeschränkte Freiheit für Ihre Nutzer

Am Flughafen, im Coffeeshop oder im komfortablen Fünf-Sterne Hotel: WLAN hat die Arbeitswelt verändert. Unabhängig von ihrem Aufenthaltsort können Ihre Mitarbeiter heutzutage überall erreichbar sein und produktiv arbeiten – zum Vorteil Ihres Geschäftes. Jedoch zu welchem Preis?

Mehr denn je stellen öffentliche Hot Spots eine Gefahr für Ihr Unternehmensnetzwerk und für die Daten Ihrer Nutzer dar. Und glauben Sie bloß nicht, auch nicht für einen Moment, dass ein passwortgeschützter Hot Spot sicherer ist. Jeder, der Zugriff auf dasselbe Netzwerk hat, ist ein potentieller Angreifer. Recherchieren Sie „Hot Spot-Hacking-Tools“: Sie werden sehen, wie einfach es tatsächlich für die Person in der Ecke ist, den Netzwerk-Traffic in der Gegend zu überwachen.

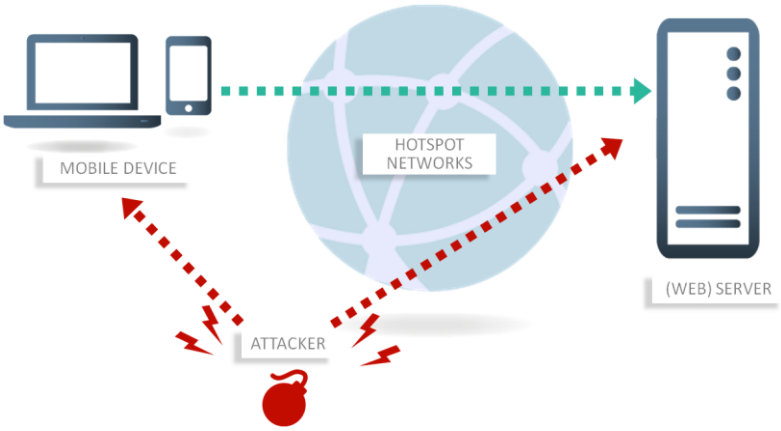
Beim Einsatz eines VPN wird der gesamte Datenverkehr Ihres Gerätes verschlüsselt. Dies ist ein erster Schritt in die richtige Richtung. Allerdings gibt es zwischen dem Start der Verbindung zum WLAN und der Verbindung zum VPN einen Moment der Verwundbarkeit. Für einen Eindringling reicht dieser Moment aus, um den am Nutzergerät eingehenden und ausgehenden Traffic zu belauschen, zu manipulieren oder sogar das Gerät selbst zu beschädigen. Letztendlich kann dies Ihrem gesamten Unternehmensnetzwerk ernsthaften Schaden zufügen.

Drei Gefahrengrade

Sämtliche Angriffe können überaus folgenschwer sein. Dennoch lassen sich diese Bedrohungen nach dem Grad ihrer Schwere (in aufsteigender Reihenfolge) in drei Kategorien eingruppieren.

Abhören des Netzwerk-Traffics

Ohne dass Nutzer das Eindringen überhaupt bemerken, könnte jemand im gleichen Zug oder Café den mit ihren Geräten gesendeten und empfangenen Datenverkehr abhören. Auf diese Weise könnte er an Unternehmensdaten und vertrauliche Informationen sowie an Nutzerzugangsdaten und persönliche Informationen gelangen. Selbst wenn solche Daten verschlüsselt sind, kann der Angreifer den Traffic speichern und für die Entschlüsselung zu einem späteren Zeitpunkt mithilfe aufwändigerer Entschlüsselungsmethoden archivieren.



NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Vier einfache Möglichkeiten, Sessions am öffentlichen WLAN zu schützen

Manipulieren des Netzwerk-Traffics

Dies ist allgemein als Man-in-the-Middle-Angriff bekannt: Eindringlinge können den öffentlichen Hot Spot hacken und den Netzwerk-Traffic umleiten. Auf diese Weise ist das Gerät anstatt mit dem öffentlichen Hot Spot in Wirklichkeit mit dem Netzwerk des Angreifers verbunden - der Nutzer bemerkt dieses Eindringen aber normalerweise nicht. Sobald eine Verbindung mit dem Nutzer besteht, kann der Eindringling den gesamten Datenverkehr abfangen, die Datenpakete ändern und modifizierte Informationen an das Endgerät schicken. Beispielsweise kann er eine E-Commerce-Website erstellen, die wie eine vertrauenswürdige Website aussieht, und darüber vertrauliche Unternehmensdaten und persönliche Informationen sammeln. Oder er kann den Nutzer zum Download einer PDF-Datei, die sich später als Malware entpuppt, auf eine andere Seite umleiten.

Natürlich werden Netzwerk-eindringlinge zunächst nach unverschlüsselten Daten suchen. Somit kann der Schutz eines VPN, welches End-to-End-Verschlüsselung bietet, die Gefahr eines Abfangens von Traffic nahezu vollständig eliminieren.

Sogar noch einfacher haben es Angreifer, wenn sie einen „falschen“ Hot Spot errichten und diesen zum Beispiel „Gast-Netzwerk“ nennen oder ihm einen Namen geben, der dem des offiziellen WLAN ähnelt. Hier ist weder Hacken noch eine spezielle Hardware notwendig: Das Netzwerk kann von einem Smartphone aus eingerichtet werden. Möglicherweise wählen mobile Nutzer dieses Netzwerk aus – vor allem, wenn der Beitritt ohne Hürden möglich ist und kein Passwort erfordert. Machen Sie als Sicherheitsexperte Ihre Nutzer auf dieses Risiko aufmerksam. Empfehlen Sie ihnen, den Netzwerknamen immer von einem Vertreter des Unternehmens, welches den Netzwerkzugriff ermöglicht, bestätigen zu lassen.

Angreifen des Endgerätes

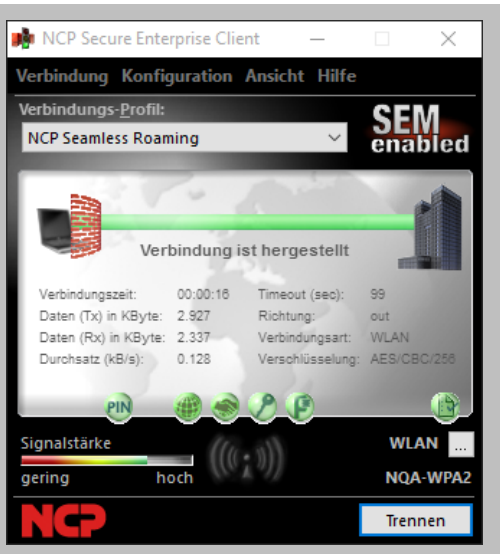
In den meisten Fällen halten eine Personal Firewall und zusätzliche Sicherheitskontrollen Angreifer davon ab, ein mit einem öffentlichen Hot Spot verbundenes Endgerät zu sabotieren. Wird jedoch die WLAN-Verbindung kompromittiert, können Angreifer möglicherweise auf das Endgerät zugreifen und dem Netzwerk-Traffic Malware anhängen. Letztendlich können sie damit eine Tür zu Ihrem Unternehmensnetzwerk öffnen. Auch wenn Ihre Mitarbeiter ein VPN nutzen und ihr Netzwerk-Traffic verschlüsselt ist, können Angreifer das VPN möglicherweise als Tunnel zum Einschleusen von Malware auf Ihre Server nutzen. Somit gefährden sie die Sicherheit von vertraulichen Unternehmensdaten und der Hardware des Unternehmens.

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Vier einfache Möglichkeiten, Sessions am öffentlichen WLAN zu schützen

Zunächst die Grundlagen

Sämtliche Lösungen in Bezug auf die Bedrohungen an öffentlichen Hot Spots beinhalten zwei wichtige Maßnahmen - die Verwendung einer Personal Firewall und die Verwendung eines VPN. Ob Sie Sicherheitsbeauftragter oder IT-Administrator sind: Sie tragen Sorge dafür, dass Ihre Mitarbeiter einen VPN-Client zum Schutz der Kommunikation zwischen Endgerät und Unternehmensnetzwerk verwenden. Um das Risiko von Angriffen einzudämmen, müssen Sie außerdem sicherstellen, dass die Personal Firewall auf den Endgeräten die Netzwerkkommunikation an öffentlichen Hot Spots einschränkt und eine Kommunikation lediglich via VPN zulässt.



Die Interaktion einer ordnungsgemäß konfigurierten Personal Firewall und einem VPN-Client dient:

- der Sicherung vertraulicher Daten
- dem Schutz des Traffics gesendeter und empfangener Daten
- der Abschirmung des Engderätes gegen Angriffe

Vier Zusatzmaßnahmen, die den entscheidenden Unterschied machen

Ein VPN und eine Personal Firewall können deutlich zur Minimierung des Risikos von Lauschangriffen und anderen Attacken beitragen. Allerdings werden Unternehmensdaten und -netzwerke noch besser geschützt, wenn zusätzlich zu den Sicherheitspraktiken an öffentlichen Hot Spots die im Folgenden beschriebenen Maßnahmen umgesetzt werden.

1. Friendly Network Detection

Eine solide Personal Firewall muss zwischen sicheren beziehungsweise „freundlichen“ Netzen – wie beispielsweise den Netzwerken im Büro, in Ihrem Rechenzentrum oder beim Nutzer zu Hause – und unsicheren öffentlichen Netzwerken unterscheiden können. Als Administrator können Sie Regeln definieren, die das richtige Sicherheitsniveau für jeden Netzwerktyp und/oder jeden Ort bieten. Zur Befolgung der Best Practices beim Mobile Computing sollten Sie die Firewall so konfigurieren, dass sämtlicher Traffic mit Ausnahme der VPN-Kommunikation an öffentlichen Hot Spots blockiert wird. Befinden sich die Nutzer in ihrem Büro oder auf dem Firmengelände, ist es unnötig, sie mit den zusätzlichen Schritten oder der Latenz eines VPN zu belasten. Folglich können Sie die Firewall so konfigurieren, dass an solchen Orten unverschlüsselter Traffic automatisch zugelassen wird.

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Vier einfache Möglichkeiten, Sessions am öffentlichen WLAN zu schützen

2. Sichere Hot Spot-Anmeldung

Möchten sich Ihre Nutzer mit einem WLAN verbinden, müssen sie normalerweise einen Browser öffnen und den allgemeinen Geschäftsbedingungen des Hot Spot-Betreibers zustimmen. Wird hingegen mittels einer ordnungsgemäß konfigurierten Personal Firewall ein unsicheres Netzwerk identifiziert, wird das Gerät den Datenverkehr ausschließlich über ein VPN erlauben. Somit wird die Hot Spot-Anmeldung blockiert.

NCP hat eine sichere und zudem einfache Möglichkeit der Nutzeranmeldung an öffentlichen Hot Spots entwickelt. Dabei bleibt die Kommunikation der Nutzer für Eindringlinge unzugänglich.

So funktioniert es:

1. Der Nutzer wählt das öffentliche WLAN aus.
2. NCPs VPN-Client stellt fest, ob das Netzwerk eine Anmeldung erfordert.
3. Ist eine Anmeldung via Browser erforderlich, öffnet der NCP-Client ein bestimmtes Browser-Fenster. Die Firewall des NCP-Clients gestattet den Zugriff ausschließlich über diesen vorgegebenen Browser. Während des Login-Prozesses ist es Nutzern nicht erlaubt, eine andere URL festzulegen oder die Optionen zu ändern. Darüber hinaus wird jede Proxy-Konfiguration ignoriert.
4. Sobald die Anmeldung erfolgt ist, erkennt der NCP-Client die Internetverbindung, baut eine VPN-Verbindung auf und blockiert erneut den gesamten übrigen Netzwerk-Traffic.

3. Network Access Control (NAC) oder Endpoint-Schutz

Sobald der VPN-Client eine Verbindung zum Netzwerk Ihres Unternehmens aufbaut, muss bestätigt werden, dass das Endgerät intakt ist. Bei Verwendung der NCP Secure Enterprise Solution kann der NCP-Client das Betriebssystem überprüfen, den Status von Sicherheits-Tools und -schutzvorrichtungen bewerten und Viren-/Malware-Scanner integrieren. Auf diese Weise kann festgestellt werden, ob Ihr Netzwerk durch eine Verbindung mit dem Endgerät gefährdet werden könnte.
Werden Auffälligkeiten registriert, schränkt der Client den Zugriff auf das VPN ein. Ist beispielsweise ein Update der Antivirensoftware auf dem Gerät notwendig, limitiert der NCP-Client den Zugriff und ermöglicht eine Verbindung lediglich zwischen dem Server für das Virenscanner-Update und dem Endgerät. Wird Malware entdeckt oder existieren andere Bedrohungen, deaktiviert der NCP-Client sofort die gesamte VPN-Verbindung und verhindert somit, dass das infizierte Gerät Ihrem Netzwerk Schaden zufügt.

4. NCP VPN Path Finder Technology

Einige Hot Spot-Betreiber gestatten lediglich das Surfen im öffentlichen Netzwerk – typischerweise DNS, HTTP und HTTPS. Zudem blockieren sie häufig Ports, die von nativen VPN-Protokollen wie beispielsweise IPsec und L2TP verwendet werden. Damit durchkreuzen sie sämtliche Bemühungen der Nutzer zur Verwendung eines VPN beim Zugriff auf ihre Unternehmensnetzwerke.

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Vier einfache Möglichkeiten, Sessions am öffentlichen WLAN zu schützen

Mithilfe der NCP VPN Path Finder Technology, erhältlich mit der NCP Secure Enterprise Solution, überwindet der NCP-Client dieses Hindernis ganz einfach. Entdeckt der VPN-Client, dass der Hot Spot native VPN-Protokolle blockiert, so wechselt er automatisch in einen modifizierten Modus (HTTPS-Emulation) und errichtet einen End-to-Site-Tunnel zum Unternehmensnetzwerk. Auf diese Weise erfolgt eine ganzheitliche, IPsec-basierte Umsetzung Ihrer unternehmensspezifischen Sicherheitsrichtlinien. Dabei sind keinerlei Aktionen seitens des Nutzers notwendig.

Zusammenfassung

Genießen Ihre Mitarbeiter die Freiheit und die Vorteile, überall dort arbeiten zu können, wo sie sich gerade befinden, so ist es für sie wichtig, die Risiken von Verbindungen über öffentliche WLAN-Netze zu kennen. Das gilt insbesondere dann, wenn sie sich mit Ihrem Unternehmensnetzwerk verbinden. Sorgen Sie dafür, dass die Mitarbeiter mit dem Vorgang zur Bestätigung des Netzwerknamens sowie den Schritten beim Zugriff auf das Netzwerk vor der Verbindung zu einem Hot Spot vertraut sind. Sorgen Sie dafür, dass sie eine Personal Firewall auf ihren Geräten aktiviert haben, die den Netzwerkzugriff an Hot Spots ausschließlich über das VPN zulässt und ansonsten verhindert. Sorgen Sie außerdem dafür, dass ihre Geräte mit einem VPN-Client ausgestattet sind – wie beispielsweise dem NCP VPN-Client (dieser beinhaltet auch eine Firewall) –, der eine einfache, sichere Hot Spot-Anmeldung sowie einen soliden Endpoint-Schutz bietet und automatisch umschaltet, wenn ein Hot Spot ein natives VPN-Protokoll blockiert.

Wollen Sie mehr über die optimale Balance zwischen Unternehmenssicherheit und Produktivität mobiler Nutzer erfahren, wenden Sie sich an **www.ncp-e.com**.

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Vier einfache Möglichkeiten, Sessions am öffentlichen WLAN zu schützen

Über den Autor

Julian Weinberger, CISSP, ist Director of Systems Engineering bei NCP engineering. Er verfügt über eine zehnjährige Erfahrung in der Netzwerk- und Sicherheitsindustrie sowie umfangreiches Fachwissen in den Bereichen SSL-VPN, IPsec, PKI und Firewalls. Julian Weinberger lebt in Mountain View, Kalifornien und ist verantwortlich für die Entwicklung von IT-Netzwerksicherheitslösungen und Unternehmensstrategien von NCP engineering. Außerdem bietet er Großkunden des Unternehmens technischen Support für ihre Remote Access-Sicherheitslösungen, sowohl vor als auch nach dem Kauf.

Über NCP engineering

Seit der Firmengründung 1986 liefert NCP engineering innovative Software. Diese ermöglicht Unternehmen, ihren Remote Access neu zu überdenken und Schwierigkeiten im Zusammenhang mit Aufbau, Verwaltung und Instandhaltung eines sicheren Netzwerkzugangs für Mitarbeiter zu beseitigen.

Mit Firmensitzen in Nürnberg, Deutschland und in der San Francisco Bay Area in Nordamerika hat das Unternehmen weltweit über 35.000 Kunden. Dazu zählen Unternehmen aus den Bereichen Gesundheitswesen, Finanzen, Bildung und Regierung sowie viele Fortune-500-Unternehmen. Zur Betreuung der Kunden hat NCP zusätzlich ein Netzwerk aus nationalen sowie regionalen Technologie-, Channel- und OEM-Partnern errichtet.

Wenn Sie mehr über NCPs Remote Access VPN-Lösungen erfahren möchten, dann besuchen Sie www.ncp-e.com.
Kontaktieren Sie NCP engineering auch über den Blog VPN Haus oder über Twitter unter @NCP_engineering.

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Vier einfache Möglichkeiten, Sessions am öffentlichen WLAN zu schützen

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und stellen keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Warenzeichen

Alle genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

Stand März 2016

Next Generation Network Access Technology

www.ncp-e.com

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com