

Neue Fortinet-Umfrage interpretiert 5G-Versprechen optimistisch

Veröffentlicht am: 30.10.2020, 11:21

Pressemittteilung von: **Fortinet** // **Constantin Funke**

Fast 90 Prozent der Befragten sehen Sicherheitskapazitäten eines Betreibers für kritisch bis sehr wichtig an

München, 30. Oktober 2020 - Fortinet (NASDAQ: FTNT), ein weltweit führender Anbieter von umfangreichen, integrierten und automatisierten Cyber-Security-Lösungen stellt die Ergebnisse einer Umfrage zu 5G vor. Die von TelecomTV in Zusammenarbeit mit HardenStance und ETSI in Auftrag gegebene Umfrage unter den Befragten aus dem Telekommunikationssektor zeigt eine weitestgehend optimistische Sichtweise auf die Umsatzchancen durch. Dies gilt allerdings nur dann, wenn die neuen 5G-Dienste sowohl sicherer als auch besser auf die wichtigsten Anwendungsfälle in Unternehmen abgestimmt sind.

5G besitzt das Potenzial, den Verbraucher- und Unternehmensmarkt anzuregen und bietet eine Reihe von Vorteilen, wie beispielsweise hohe Geschwindigkeiten, geringere Latenzzeiten und mehr Bandbreite. Die fünfte Generation des Mobilfunkstandards ebnet auch den Weg zu Verbesserungen in Bereichen wie etwa dem Gesundheitswesen, dem Autonomen Fahren oder Smart Cities - überall dort, wo durch neue Nutzungsmöglichkeiten das tägliche Leben verbessert werden kann. Darüber hinaus erhöht 5G die Anzahl der verbundenen Geräte beträchtlich, was ein neues profitables Feld für Cyber-Kriminelle darstellt. Vor diesem Hintergrund müssen Mobilfunknetzbetreiber und Unternehmen eine starke Cyber-Sicherheitsstrategie haben, die ihre gesamte Infrastruktur durchgängig schützen kann.

Eine gute Geschäftsgelegenheit

Insgesamt erwarten fast 90 Prozent der Befragten ein Wachstum des durchschnittlichen Umsatzes pro Nutzer (Average Revenue per User; kurz: ARPU) aus ihren Investitionen. Es wird erwartet, dass sich dieses Wachstum gleichmäßig auf öffentliche und private 5G-Netze verteilt. Da aber mindestens die Hälfte aller privaten Netze wahrscheinlich von den Betreibern eingerichtet und verwaltet werden, könnten solche Unternehmen potenziell bis zu 75 Prozent des gesamten 5G-Geschäfts erobern.

Entscheidend für die Erzielung dieser Gewinne ist jedoch nach Ansicht von 64 Prozent der Befragten die Erhöhung der bestehenden Sicherheit - sowohl in Bezug auf die Architektur als auch auf den Betrieb. Darüber hinaus ist die Anpassung von Lösungen an spezifische Business-Anwendungsfälle für fast drei Viertel der Befragten entweder kritisch oder sehr wichtig - insbesondere in den vertikalen Schlüsselmärkten Transport, Logistik, Automatisierung, Fertigung und Gesundheitswesen.

Das bedeutet: Alte Geschäftsmodelle der Bereitstellung undifferenzierter mobiler Verbindungen werden nicht mehr ausreichen. Um erfolgreich zu sein, werden die meisten Anbieter Partnerschaften mit anderen Providern sowie mit ihren Unternehmenskunden in gemeinsamer Verantwortung eingehen müssen.

Kooperationen zwischen den Anbietern sind für die Umfrageteilnehmer wichtig: 44 Prozent der Befragten sehen Cloud-Anbieter als Partner, oder zumindest hauptsächlich als Partner, während nur 11 Prozent sie als reine Konkurrenten betrachten.

Diese Ergebnisse decken sich mit der bestehenden Verantwortungsteilung zwischen Cloud-Anbietern

und ihren Unternehmenskunden: Wartung und Sicherheit der Infrastruktur obliegt dem Anbieter, während das Unternehmen Daten und Anwendungen selbst sichern muss.

Starkes Sicherheitskonzept gefragt

Cyber-Sicherheit ist für den Großteil der Befragten in Bezug auf 5G wichtig. Mehr als 80 Prozent der Umfrageteilnehmer sind der Ansicht, dass die inhärenten Sicherheitsmerkmale der Spezifikationen des 5G 3rd Generation Partnership Project (3GPP) eine Richtlinie für den 5G-Markt darstellen. 62 Prozent geben an, dass einige oder die meisten 5G-Anwendungsfälle zusätzliche Sicherheitsmerkmale erfordern werden.

Viele fordern ein Qualitätsversprechen, das über die reine Konnektivität hinausgeht und das den erhöhten Sicherheitsanforderungen von 5G und den verschiedenen Anwendungsfällen angemessen Rechnung trägt. Fast 90 Prozent erwähnen dies als sehr wichtig. Denn 61 Prozent der Befragten halten ein Geschäftswachstum im ARPU für unwahrscheinlich, wenn es sich hauptsächlich oder vollständig auf die Verbindungsschicht der 5G-Wertschöpfungskette beschränkt.

Ronen Shpirer, Director Solutions Marketing bei Fortinet, sagt: "Die Migration der heutigen Mobilfunknetze zu 5G verlangt eine neue Form der Security. Zum virtualisierten, verteilten und dynamischen Natur des 5G-Kerns kommt die massive Steigerung der Skalierbarkeit, die zunehmende Nutzung von Multi-Access Edge Computing (MEC) sowie der konkrete, kritische Anwendungsfall hinzu. Diese Kombination erfordert eine starke Security für die zugrunde liegende Infrastruktur und jeden einzelnen Business-Anwendungsfall. Hier zeigt der nachweisliche Erfolg von Fortinet bei der Bereitstellung von Sichtbarkeit und Schutz, Skalierbarkeit und Preis-Leistungs-Verhältnis bei 4G- und 5G-Carrier-Grade-Benutzer- und Steuerungsebenen einen klaren Vorteil für diejenigen, die von diesen neuen 5G-Möglichkeiten profitieren wollen."

5G und die Ausweitung der Cyber-Bedrohungslandschaft werden mobile Netzbetreiber und Unternehmen dazu veranlassen, einen ganzheitlichen Sicherheitsansatz zu verfolgen, um mit dieser sich dynamisch entwickelnden Umgebung Schritt zu halten.

Methodik

In der TelecomTV-Umfrage im Auftrag von Fortinet wurden die Befragten aus dem Telekommunikationssektor weltweit nach ihrer Sicht der Entwicklung des 5G-Marktes für Unternehmensdienste sowie nach den Sicherheitsanforderungen und Sicherheits-Geschäftsmodellen gefragt, die zur Unterstützung dieser Unternehmensdienste erforderlich sind. Mehr als ein Drittel der Befragten sind Netzbetreiber/Service Provider, einschließlich der großen globalen Tier-1-Mobilfunknetzbetreiber. Ein weiteres Viertel sind Anbieter von Hardware-/Softwaresystemen.

Über Fortinet

Fortinet (NASDAQ: FTNT) schützt die wertvollsten Ressourcen einiger der größten Unternehmen, Service Provider und Behörden weltweit. Wir bieten unseren Kunden vollständige Transparenz und Kontrolle über die sich ausweitende Angriffsfläche sowie die Möglichkeit, heute und in Zukunft immer höhere Leistungsanforderungen zu erfüllen. Nur die Fortinet Security Fabric-Plattform kann die kritischsten Sicherheits Herausforderungen bewältigen und Daten in der gesamten digitalen Infrastruktur schützen, ob in Netzwerk-, Anwendungs-, Multi-Cloud- oder Edge-Umgebungen. Fortinet ist Nummer 1 bei den weltweit am häufigsten ausgelieferten Security Appliances. Mehr als 465.000 Kunden vertrauen Fortinet den Schutz ihrer Marke an. Das Fortinet Network Security Expert (NSE) Training Institute ist sowohl ein Technologie- als auch ein Schulungsunternehmen und verfügt über eines der größten und umfangreichsten Cyber-Security-Trainingsprogramme der Branche. Weitere Informationen dazu auf

<https://www.fortinet.com/de>, dem Fortinet Blog oder bei den FortiGuard Labs.

Pressekontakt:

Akima Media

Alexandra Krohn / Christina M. Rottmair

Garmischer Str. 8

80339 München

Tel.: +49 (0) 89-1795918-0

fortinet@akima.de

www.akima.net

Pressekontakt

Herr Constantin Funke
PR-Beauftragter

Fortinet

Maximilianstr. 13
80539 München, Deutschland

Telefon: +49 (0) 89-1795918-0

E-Mail: fortinet@akima.de

Website:

Firmenportrait

Fortinet (NASDAQ: FTNT) schützt die wertvollsten Ressourcen einiger der größten Unternehmen, Service Provider und Behörden weltweit. Fortinet stattet seine Kunden mit intelligenten, lückenlosen Schutzmaßnahmen gegen das rasant wachsende Cyber-Bedrohungsumfeld aus und ermöglicht es den permanent steigenden Leistungsanforderungen am Borderless Network entgegenzuwirken. Nur die Fortinet Security Fabric-Architektur kann umfassende IT-Security ohne Kompromisse garantieren, die alle Security-Anforderungen von Netzwerk-, Applikations-, Cloud- oder Mobile-Umgebungen adressiert und berücksichtigt. Fortinet liefert die meisten Security Appliances weltweit aus. Mehr als 385.000 Kunden vertrauen Fortinet den Schutz ihrer Marke an. Mehr dazu auf: www.fortinet.de, im Fortinet Blog, oder bei den FortiGuard Labs, eines der besten Forschungs- und Analyse-Teams für IT-Bedrohungen weltweit.

Wichtiger Hinweis:

Für diese Pressemitteilung sowie das Bild- und Tonmaterial ist allein der jeweils angegebene Herausgeber verantwortlich. In der Regel ist dieser der Urheber der Presstexte sowie der angehängten Bild und Informationsmaterialien. Das TRENDKRAFT-Pressportal ist für den Inhalt dieser Pressemitteilung nicht verantwortlich und übernimmt keine Haftung für die Korrektheit oder Vollständigkeit der dargestellten Meldung. Die Nutzung von hier archivierten Informationen zur Eigeninformation und redaktionellen Weiterverarbeitung ist in der Regel kostenfrei. Vor der Weiterverwendung sollten Sie allerdings urheberrechtliche Fragen mit dem angegebenen Herausgeber klären. Eine systematische Speicherung dieser Daten sowie die Verwendung auch von Teilen dieses Datenbankwerks sind nur mit schriftlicher Einwilligung durch das TRENDKRAFT-Pressportal gestattet.

Des Weiteren beachten Sie bitte unseren Haftungsausschluss unter: <https://trendkraft.io/haftungsausschluss>