MSP
Barracuda
Your journey, secured.

Herausforderungen für MSPs in Zeiten von Corona und wie Sie als IT-Systemhaus damit fertig werden!

Die Corona-Krise zwingt Unternehmen weltweit zu drastischen Maßnahmen. Arbeit im Home Office ist nun kein Sonderfall mehr, sondern gehört vielerorts zum Alltag. Innerhalb kürzester Zeit muss die Wirtschaft auf die neuen Herausforderungen reagieren. Trotzdem sind noch lange nicht alle Unternehmen bereit dafür. Dieses Whitepaper verrät, welche Herausforderungen nun auf Sie als Managed Service Provider und Ihre Endkunden zukommen und wie Sie damit fertig werden.

WHITE PAPER

Mit MSPs durch die Krise

April 2020: Die **Corona-Krise** hat Auswirkungen auf alle Bereiche des täglichen Lebens. Auch der Unternehmensalltag in der DACH-Region ist betroffen: Einer aktuellen **Bitkom-Studie** zu Folge arbeitet bereits jetzt **jeder zweite Arbeitnehmer** von zu Hause [1]. In den kommenden Wochen dürften es noch mehr werden. In vielen Unternehmen wurden die neuen Arbeitsregelungen allerdings hastig und mit wenig Vorbereitung eingeführt. Selbst dort, wo Home Office bislang gewährt wurde, stellt dieser Schritt eine **radikale Entscheidung** dar. Wo bislang nur manche Mitarbeitergruppen an einzelnen Tagen von zu Hause aus arbeiten konnten, werden nun flächendeckend beinahe alle Arbeitnehmer in die Heimarbeit geschickt. Wenig überraschend darum, dass sich laut der Bitkom-Studie fast **40 Prozent der Mitarbeiter** nicht ausreichend für eine Arbeit im Home Office gerüstet sieht.

In der Tat stellt die aktuelle Situation Unternehmen vor **gewaltige Herausforderungen:** Unstrittig ist, dass der **gesundheitliche Schutz** der Mitarbeiter und die Eindämmung des Virus an erster Stelle stehen muss. Gleichzeitig muss die **Arbeit im Unternehmen** weitergehen. Einen kleinen Bonus dabei haben nun solche Unternehmen, die frühzeitig die Chancen der Digitalisierung genutzt haben und sowohl **Infrastruktur**, als auch **Prozesse** für erfolgreiche mobile Arbeit etabliert haben. Nun sind **Managed Service Provider** gefragt, auf die Zeit der Krise mit kreativen und flexiblen Lösungen für ihre Kunden zu reagieren. Sie übernehmen die **Wartung der Infrastruktur** aus der Ferne und sorgen damit für eine **sichere und stabile Infrastruktur** für die Arbeit im Home Office. **Remote Monitoring und Management**, sowie **Cloud Security & Backup** können dabei helfen. So werden auch in Infrastruktur-belastenden Krisenzeiten **produktive und sichere Arbeitsumgebungen** sichergestellt.

In diesem Whitepaper erfahren Sie

- **welche Herausforderungen** die aktuelle Corona-Krise für Managed Service Provider bereit hält.
- **was Sie tun können**, um Unternehmen für die nächste Zeit fit zu machen.
- wie **Remote Monitoring und Management sowie Cloud Security & Backup** dabei helfen können, Managed Service Provider bei ihrer täglichen Arbeit zu unterstützen.

[1] https://www.adzine.de/2020/03/home-office-in-zeiten-von-corona-jeder-zweite-arbeitnehmer-schon-zuhause/

Herausforderungen im Corona-Alltag

Managed Service Provider in der DACH-Region haben durch die Corona-Krise mit den vielfältigen Herausforderungen Ihrer Kunden zu kämpfen. Dazu gehören **Probleme mit dem Netzwerk, technische Herausforderungen** und wachsende **Security Bedenken**.

1. **Internetgeschwindigkeit und Stabilität**
   Die gegenwärtige Situation stellt die Wirtschaft in der DACH-Region auf vielfältige Art und Weise auf die Probe:
   Viele Unternehmen setzen VPN-Verschlüsselungen bei der Heimarbeit ein, um eine Verbindung zum Firmennetz herzustellen. Die sind allerdings nicht zwangsläufig auf den **aktuellen massiven Anstieg an Nutzern** ausgelegt. In vielen Unternehmen sind darum **Engpässe** zu erwarten. Die Folge: **Verzögerungen bei der Arbeit und sinkende Produktivität**.

2. **Technische Herausforderungen**
   Eine nicht zu vernachlässigende Hürde stellt bereits die notwendige **technische Ausstattung** dar. Diese Herausforderung beginnt bei der **Bereitstellung geeigneter Hardware**. Wenn Unternehmen ihre Arbeitsabläufe komplett in die Heimarbeit verlagern, ist ein entsprechend **geeignetes Equipment** unabdingbar. Gerade darauf sind viele Unternehmen aber nicht vorbereitet: Mitarbeiter, die bisher an stationären PCs beschäftigt waren, benötigen nun **mobile Endgeräte** für den Heimeinsatz. Dieses ist nicht zwangsläufig in ausreichender Menge im Unternehmen vorhanden. Für MSPs kann es in diesen Zeiten schwierig sein, den **Überblick** über alle im Netzwerk angeschlossenen Geräte und Software-Lösungen zu behalten.
   Wenn die Geräte vorhanden und eingerichtet sind, können bestimmte für die Heimarbeit notwendige **Benutzeroberflächen** von Heimarbeitstools (Remote Desktop, VPN) für **Verwirrung** sorgen. Ist das zuständige IT-Team in solchen Fällen unter Umständen schwer zu erreichen, kann das zu **Verzögerungen in der Produktivität** führen.

3. **Security-Bedenken und Endpoint Security**
   Wenn sich die Kommunikation immer mehr in den digitalen Raum verlagert, steigen die Chancen, dort **Opfer eines Cyberangriffs** zu werden. Viele Unternehmen sind besorgt, dass Heimnetzwerke ihrer Mitarbeiter nicht genügend gegen Angriffe von außen ausgerüstet sein könnten: Oft werden kritische Updates für Betriebssysteme oder verwendete Updates gar nicht oder viel zu spät installiert. Das kann Cyberkriminellen Tür und Tor öffnen.
   Und in der Tat nutzen Cyberkriminelle bereits die aktuelle Situation für besonders **perfide Angriffe** aus. Beispielsweise wurden Fälle öffentlich, in denen **Phishing-Mails** mit „Informationen zu Corona“ warben. Dabei wurden sogar die Namen von seriösen Institutionen wie der WHO genutzt, um die Mail mit dem schädlichen Anhang entsprechend zu tarnen.
   MSPs stehen darum nun vor der Herausforderung, einen **einheitlichen Sicherheitsstandard** der genutzten Geräte ihrer Endkunden sicherzustellen.

Absetzung als Kasten („Zwischen-Fazit“)
Diese Probleme werden aktuell also an MSPs herangetragen

- Mitarbeiter müssen mit praxistauglichen Geräten ausgestattet werden.
- Alle Geräte müssen gegen Cyberangriffe gerüstet werden.
- Einrichtung und Konfiguration müssen ohne direkten Kontakt und per Fernwartung durchgeführt werden.
- Aufwendungen und Leistungen müssen lückenlos dokumentiert werden.

Cloudlösungen und eine Verwaltung aus der Ferne können hier wertvolle Hilfe sein!

Ende Kasten

Lösungen

Glücklicherweise sind Managed Service Provider der aktuellen Krisensituation nicht schutzlos ausgeliefert. Es gibt eine **Reihe von Empfehlungen** und **wirksamen Strategien**, auf die sie jetzt zurückgreifen können, um der Lage Herr zu werden.

1. **Überblick über die Hardware herstellen**
   Wenn Engpässe bei der genutzten Hardware-Ausstattung zu erwarten sind, greifen Unternehmen auf **kreative „Out of the Box"-Ansätze** zurück: Geräte aus dem regulären Betrieb werden mit ausgemusterter Hardware aus dem Lager und BYOD ergänzt. Damit MSPs trotzdem den **Überblick behalten**, sollten sie auf geeignete Wartungsplattformen zurückgreifen. **Remote Monitoring und Management** (RMM)-Lösungen können hier unterstützend hinzugezogen werden. So können über zentrale Dashboards alle Geräte jederzeit im Blick behalten werden.

2. **Konnektivität sichern**
   Tests der IT-Teams verraten, ob die im Unternehmen genutzte **VPN-Verbindung** zum Netzwerk für einen großflächigen Zugriff von Mitarbeitern aus dem Home Office geeignet ist. Gegebenenfalls sollten jetzt **Serverkapazitäten aufgestockt** und **zusätzliche Lizenzen** erworben werden, um allen Angestellten Ihrer Endkunden Zugriff aus dem Home Office zu ermöglichen.

3. **Cloud Monitoring & Management**
   Die Arbeit in der Cloud gehört in vielen Unternehmen bereits seit längerer Zeit zum Alltag. Wenn geteilte Arbeitszimmer und Schreibtische wegfallen, wird ein **gemeinsamer digitaler Arbeitsraum** bei Ihren Kunden aber unabdingbar. Auch kleine und mittelständische Unternehmen nutzen bereits Google Docs oder Dropbox. Oft fehlt allerdings eine **zentrale Absicherung**. Hier kann eine externe Remote Management und Monitoring Plattform helfen, alle Cloud-Anbindungen im Blick zu behalten. Der **Schutz der Cloud-Speicher** vor Cyberbedrohungen sollte dabei genauso sichergestellt werden wie **Backup-Funktionen** zum Schutz der Daten.

4. **Meetings nur noch online**
   Die gegenwärtigen Empfehlungen zur Corona-Krise zielen auf einen weitestgehenden **Verzicht jeglicher Face-To-Face Kommunikation** ab. Davon betroffen sind natürlich auch sämtliche Formen von Business-Meetings, Konferenzen und Kundengesprächen. Glücklicherweise gibt es eine ganze Reihe **digitaler Konferenzräume**, die nun Abhilfe schaffen: **GoToMeeting, Google Hangouts** oder **Zoom** können die Lücke bis zum nächsten persönlichen Treffen überbrücken. Teilweise sind **kostenfreie Versionen** verfügbar, die bei Bedarf erweitert werden können.

5. **Sicherheit hat Priorität**
   Die veränderte Situation im Arbeitsalltag Ihrer Endkunden führt zu **steigenden Sicherheitsanforderungen** bei MSP-Dienstleistern. Doch Home Office muss nicht zwangsläufig ein größeres Sicherheitsrisiko darstellen, als die Arbeit im Büro. In jedem Fall sind aber Sicherheitsempfehlungen zu beachten und gegebenenfalls die Mitarbeiter Ihrer Endkunden zu sensibilisieren. Eine ganze Reihe von Sicherheitstipps hilft dabei, Unternehmensdaten auch von daheim so gut wie möglich zu schützen:

- Ein **ganzheitliches Sicherheitskonzept** garantiert, dass alle Prozesse einheitlich aufgesetzt werden.
- Eine **Begrenzung von Zugriffsrechten** limitiert von Anfang an potenzielle Einfallstore für Cyberkriminelle.
- **VPN-Verschlüsselung** sollte den Datenverkehr im Unternehmensnetz schützen. Die Verschlüsselung sorgt dafür, dass Daten nicht mehr von außerhalb einsehbar sind.
- Eine **Firewall** schirmt die Rechner zusätzlich vor Angriffen von außen ab.
- **Aktiver Virenschutz** sollte eine Selbstverständlichkeit sein, damit Bedrohungen, die beispielsweise in infizierten E-Mails verschickt werden, möglichst früh erkannt werden.
- Alle **aktuellen Updates** des Betriebssystems und der verwendeten Software sollten jederzeit auf dem aktuellen Stand gehalten werden, damit Schwachstellen so bald möglich geschlossen werden können.
- Mitarbeiter sollten dafür sensibilisiert werden, auch die **privaten Heimnetzwerke abzusichern** und nicht auf die Werkeinstellung ihres Routers zu vertrauen.
- **Notfallpläne** für **räumlich getrennte Teams** helfen dabei, auch in schwierigen Situationen die Kontrolle zu behalten.

Remote Management kann MSPs dabei helfen, die Sicherheitsanforderungen ihrer Kunden umzusetzen.

Nutzen Sie Expertenwissen

Die Herausforderungen für die deutsche Wirtschaft in der Corona-Krise sind vielfältig. Managed Service Provider müssen nun auf diese speziellen Anforderungen der Wirtschaft reagieren und für die Etablierung neuer Prozesse und die Einrichtung digitaler Arbeitsplätze geeignete Lösungen finden. Bei der Bewältigung dieser Aufgaben können Remote Management und Monitoring sowie Cloud Security & Backup Lösungen helfen. Ein **Partner mit dem geeigneten Expertenwissen** ist Barracuda MSP, die für MSP zuständige Geschäftseinheit von Barracuda Networks. Barracuda MSP unterstützt Managed Service Provider dabei, passende Lösungen für ihre Kunden zu finden. Dazu gehören das Bereitstellen von Expertenwissen und Ressourcen sowie zuverlässiger und skalierbarer MSP-Lösungen.

Barracuda Essentials for Office 365 – MSP

Es gibt in Unternehmen eine Reihe digitaler „Standardprozesse“, die in jedem Fall besonders abgesichert sein sollten. Dazu gehören sämtliche Office-Anwendungen aus dem Business-Alltag. Barracuda Essentials for Office 365 ist eine umfangreiche MSP-Lösung, die dabei helfen kann und deren intuitive Benutzeroberflächen flüssige Arbeitsprozesse sicherstellen. Im Kern stellt sie mehrstufige Security Archivierungs- und Datenschutz-Funktionen für Office 365-Umgebungen zur Verfügung.

Dazu gehören:

- **Cloud-to-Cloud-Backup** schützt E-Mail-Postfächer und Cloud-Speicher vor Datenverlusten bei menschlichen Fehlern oder Cyberangriffen.
- **Barracuda MSP E-Mail Security Service** sorgt für einen sorgenfreien Mail-Austausch und schützt das Netzwerk schon vor dem Gateway vor Eindringlingen. Nach dem Gateway werden die Rechner Ihrer Endkunden mit einer intelligenten KI direkt in der Mailbox abgesichert.
- **Barracuda Cloud E-Mail Archiving Service** hilft bei der Einrichtung eines Cloud-basierten Archivs in dem E-Mails und Daten durch vielfältige indizierungs- und Suchoptionen auch über einen längeren Zeitraum hinaus zugänglich gemacht werden können.

Barracuda Managed Workplace

Barracuda Managed Workplace ist eine umfassende, mandantenfähige Plattform für Remote Monitoring & Management (RMM) mit leistungsstarken, integrierten Sicherheitstools und Diensten für MSPs. Komplettes Remote Monitoring und Management durch Fernwartung wird mit dem Barracuda Managed Workplace für MSP IT-Dienstleister möglich. Ein zentrales Dashboard übernimmt dabei die Verwaltung und Wartung aller Geräte. So behalten MSPs die Übersicht über alle im Kundennetzwerk angeschlossenen Geräte – egal ob sie sich im Bürogebäude oder im Home Office befinden. Mittels Fernverbindung zu den Rechnern der Kunden werden Probleme umgehend identifiziert und entsprechende Lösungen gefunden. Dadurch bekommen MSPs die Möglichkeit, Schwachstellen zu bewerten, Einfallstore für Cyberkriminelle zu schließen, den normalen Betrieb zu sichern und die Wiederherstellung von Daten nach einem Angriff zu gewährleisten.

Folgende Funktionen stehen dafür zur Verfügung:

- **Aktiver Virenschutz** wird bereitgestellt, überwacht und entsprechend der Anforderungen der Infrastruktur konfiguriert.
- Alle Systeme werden **laufend überprüft** und Online-Bedrohungen abgewehrt. Security-Vorfälle werden analysiert und Berichte über abgewehrte Bedrohungen übermittelt.
- Alle verfügbaren **Updates** werden bei Verfügbarkeit sofort installiert und deren Funktionstüchtigkeit anschließend überprüft.

Darüber hinaus verfügt der Barracuda Managed Workplace über einige zusätzlich integrierte Funktionen:

- Der **Barracuda Content Shield** ist eine Cloud-verwaltete Sicherheitslösung inklusive Inhaltsfilter, der Schutz vor bösartigen Websites, unangemessenen Inhalten und gefährlichen Dateianhängen bietet.
- **Intronis Backup** ist eine Software-Backup- und Disaster-Recovery-Lösung mit sicheren hybriden lokalen und Cloud-Backup-Diensten, der effektiven Schutz vor Dateiverlusten sicherstellt.

Haben Sie noch Fragen zu den Herausforderungen, die auf Unternehmen während der Corona-Krise zukommen?

Vereinbaren Sie mit uns ein Live-Webinar!

Mario Becker | mbecker@barracuda.com
Kevin Sivananthan | ksivananthan@barracuada.com
0157-35992801

MSP Barracuda
Your journey, secured.