MCL

HOW TO MANAGE IT.

HANDBUCH

WAS JETZT WICHTIG IST.

RISIKOMANAGEMENT & SOFORTMASSNAHMEN

INHALTSVERZEICHNIS

1 VORWORT: EINEN KÜHLEN KOPF BEWAHREN

Nicht nur mittelständische Unternehmen haben die Auswirkungen einer möglichen Pandemie auf Geschäftsmodelle oder Dienstleistungen nicht im Blick gehabt. Allein die Verfügbarkeit der IT-Landschaft sicherzustellen, ist für viele Unternehmen aktuell eine Herausforderung. Flexibilität und Schnelligkeit stehen bei den geforderten Sofortmaßnahmen seitens der Geschäftsführung im Vordergrund. Wer von heute auf morgen die Hälfte seiner Belegschaft zu Homeoffice-Usern macht, sollte nicht überstürzt, sondern besonnen mit den richtigen Maßnahmen planen und handeln. Denn auch Abhängigkeiten und Nebeneffekte sind dabei zu berücksichtigen.

Wir möchten in diesem Dokument unsere Erfahrungen aus IT-Projekten sowie unsere Einschätzungen von Maßnahmen teilen, die wir genauso wie unsere Kunden bereits treffen mussten. Diese Handlungsempfehlungen sollen Sie bei der individuellen Entscheidungsfindung unterstützen, selbst wenn Sie sich bisher nicht mit Risikomanagement oder IT-Governance beschäftigt haben.

Christian Priske
Leiter Netzwerk & Security bei MCL

Springen Sie direkt ins Kapitel » Soforthilfe «, um vorbereitete Lösungen der MCL einzusehen.

2 KURZFRISTIGE MASSNAHMEN

Spätestens, nachdem die WHO das Coronavirus zur Pandemie erklärt hat, haben die meisten Unternehmen gehandelt. Doch die teils weitreichenden Folgen dieser Sofortmaßnahmen können wiederum zu neuen IT-Herausforderungen führen.

2.1 Typische Maßnahmen

- Separation von Mitarbeitern zur Gewährleistung der Verfügbarkeit von Abteilungen und Geschäftsprozessen trotz möglicher Infektion einzelner Mitarbeiter.
- Mitarbeiter mit Notebooks werden angehalten, von zu Hause zu arbeiten.
- Kurzfristige Anschaffung zusätzlicher Notebooks, um weitere Mitarbeiter ins Homeoffice schicken zu können.
- Unternehmen, die mit Remote-Desktop und VDI-Lösungen arbeiten, weiten diese für Heimarbeitsplätze aus. Die ThinClient- und Serverlandschaft wird zur Deckung des erwarteten Bedarfs erweitert.

2.2 Folgen

Natürlich nehmen Datenzugriffe von außen zu. Wer den kompletten Datenverkehr seiner Homeoffice-User nun per VPN ins eigene On-Prem-Rechenzentrum tunnelt, stößt schnell an Kapazitätsgrenzen.

- Möglicherweise ist der Firewall-Cluster zu klein dimensioniert, um alle Verbindungen zu terminieren.
- Es fehlen Client-Zertifikate, Lizenzen für VPN-Clients oder Endpoint-Protection- Clients.
- Die Leitungskapazität reicht nicht aus und der Provider kann nicht ausreichend skalieren.
- Es stehen nicht ausreichend mobile Endgeräte oder ThinClients für Mitarbeiter zur Verfügung.

- Die Rufumleitung der Telefonanlage sprengt die Anzahl möglicher Verbindungen, Mitarbeiter sind sporadisch nicht erreichbar.
- Einige Dienste sind von außerhalb nicht erreichbar, da dies bisher nie erforderlich war.
- Der ungewohnte Umgang mit VPN-Client oder Softphone beeinträchtigt Arbeitsfähigkeit und Effizienz mancher Kollegen im Homeoffice.

2.3 Empfehlungen

Erreichbarkeit

Priorisieren Sie wichtige Dienste, Applikationen und Nutzer vor unkritischen und weniger wichtigen Diensten. (Dynamisches Bandbreiten-Management auf Layer 7, 8)
Überwachen Sie die Auslastung der WAN-Anbindung, die maximale Session-Anzahl, Kapazitätsgrenzen wie CPU Last und RAM. Setzen Sie Schwellenwerte, um gezielt reagieren zu können.
Prüfen Sie, wie viele Telefonverbindungen nach extern möglich sind. Denn bereits bei der einfachen Rufumleitung werden ggfs. zwei Leitungen belegt. Sprechen Sie mit Ihrem Provider und nutzen Sie ein Softphone, wo möglich. Stellen Sie den Mitarbeitern Headsets für zu Hause zur Verfügung. Prüfen Sie Ihre Telefonanlage hinsichtlich der Anforderungen. Collaboration-Lösungen wie Skype, MS Teams, Zoom und Co. können dabei entlasten. Outlook WebExchange/Anywhere benötigen wenige zentrale Anpassungen und lassen Mailzugriff von nahezu beliebigen Endgeräten via Web-browser zu.

Sicherheit

Prüfen Sie das Regelwerk Ihrer Firewall und DMZ für den veränderten Bedarf, um Dienste auch von außerhalb verfügbar zu machen (Ports, Policies).
Schaffen Sie individuelle Wartungszugänge mit separatem oder besser personalisiertem User und PW für interne und externe Experten, damit im Falle eingeschränkter Einsatzfähigkeit Ihrer IT schnelle Hilfe von extern auch remote möglich ist.
Stellen Sie sicher, dass Dokumentationen wie Notfallpläne trotz Ausfall von Einzelpersonen auffindbar und durchführbar sind.

BYOD bekommt ggfs. erstmals Relevanz, um Mitarbeitern den Zugang über private Endgeräte per SSL oder Remote-Desktop zu ermöglichen.
Achten Sie gerade jetzt verstärkt auf unternehmensfremde Personen, die sich auf Ihrem Firmengelände aufhalten.

Investitionen

Nehmen Sie sich trotz der Umstände etwas Zeit, um beispielsweise unterschiedliche Lösungen für **mobiles Arbeiten** auf Ihren konkreten Bedarf hin zu prüfen.
Mögliche Parameter finden Sie in diesem Dokument.

Prozesse

Nutzen Sie eine Softwareverteilung, um idealerweise noch vor dem Einsatz im Homeoffice wichtige Applikationen auf den erforderlichen Geräten verfügbar zu machen.
Schreiben Sie kleine Anleitungen und informieren Sie die Mitarbeiter, wie sie sich richtig von außerhalb einwählen und telefonieren können. Entlasten Sie Ihr Helpdesk mit Infos zu vorhersehbaren und somit planbaren Support-Fragen, die sich nicht gänzlich vermeiden lassen.
Schichtbetrieb ist eine kurzfristige Maßnahme zur Überbrückung von Auslastungsspitzen, um IT-Ressourcen nicht über die Kapazitätsgrenze hinaus zu belasten.
Mangels Kinderbetreuung können viele Eltern so auch bei Heimarbeit effektiver arbeiten.

Cloud-Dienste

Die aktuell besonderen Anforderungen genauso wie künftige Peaks im Alltagsgeschäft können Sie durch den Einsatz von Kapazitäten aus der Cloud überbrücken.
Neben Rechenleistung und Speicher lassen sich auch ganze Dienste verlagern.
Sie verdoppeln damit kurzfristig Ihre Ressourcen ohne CAPEX und langfristige Bindung.
Entspannt sich die Lage, können Sie nach Wunsch die Cloud-Services kündigen und die Daten zurück in Ihr Rechenzentrum holen.

3 SOFORTHILFE

Hier finden Sie Soforthilfe für drei aktuelle Herausforderungen:

- Es fehlt Ihnen an mobilen Endgeräten für die Arbeit von zu Hause?
- Sie haben ausreichend PCs und Notebooks zur Verfügung, aber diese sind für die Heimarbeit nicht gerüstet?
- Ihre zentrale IT Infrastruktur bzw. Ihre Ressourcen sind für den derzeitigen Bedarf nicht ausgelegt?

Unsere Soforthilfe-Bundles finden Sie im MCL Shop.

3.1 Keine mobilen Endgeräte?

„Es fehlt Ihnen an mobilen Endgeräten für die Arbeit von zu Hause?"

Noch bevor die Verfügbarkeit am Markt drastisch eingebrochen ist, hat MCL den Lagerbestand gezielt erhöht. Im Hinblick auf den Bedarf haben wir Produktpakete bestehend aus Notebooks, Clients, Monitoren, Headset und Peripherie für Sie zusammengestellt – diese sind ab Lager verfügbar, solange der Vorrat reicht.
BLOG BEITRAG / SHOP

Um Sie noch weiter zu entlasten, liefern wir Ihnen die gewünschten Produkte auch bereits betriebsfertig. Im Rahmen unseres **Factory Service** übernehmen wir die Softwarebetankung nach individuellen Vorgaben und spielen nötige Patches und Treiber auf. Mittels Remote-Zugriff auf unseren Fileserver geht die Bereitstellung sehr schnell. Auch die Remote-Anbindung an Ihr Unternehmen lässt sich so vorab mit einem Test-User überprüfen. Die Ware kann also direkt dahin, wo sie gebraucht wird.
Und Sie sparen wertvolle Zeit.

3.2 Ready for Homeoffice?

„Sie haben ausreichend PCs und Notebooks zur Verfügung, aber diese sind für die Heimarbeit nicht gerüstet?“

Unsere **Aruba Remote Access Points** können von Ihren Mitarbeitern mittels Plug-and-play zu Hause installiert werden, nachdem wir mit Ihnen die zentralen Anpassungen vorgenommen haben. Damit lassen sich sogar ThinClients und Desktop-Rechner anschließen, die nicht mit Software und Setup für den Einsatz von extern ausgelegt sind. Endgeräte agieren wie im Netzwerkbetrieb, Sicherheitsanforderungen und Verbindungsaufbau werden vom Remote AP abgedeckt. Auch Drucken und Telefonieren sind weiterhin möglich. Das Schreibtischtelefon kann direkt per PoE mit Strom versorgt werden. Jeder Client kann sich kabelgebunden oder drahtlos sicher von zu Hause ins Firmennetz einloggen.

Unser **Security Gateway** bietet bis auf kleine Unterschiede eine ähnliche Funktionalität wie Remote Access Points. Die enthaltene vollwertige IDS/IPS-Firewall filtert Anwendungen wie Office365 und ermöglicht, lokal am Heimarbeitsplatz ins Internet „auszubrechen“. Dies verhindert Flaschenhälse in Ihrem Rechenzentrum.
Setzen Sie Aruba, Fortinet oder Sophos zentral als Firewall bzw. SD-WAN-Router ein, ergeben sich daraus weitere Möglichkeiten in der Konfiguration und Verwaltung.
Eine zwingende Voraussetzung ist dies jedoch nicht.

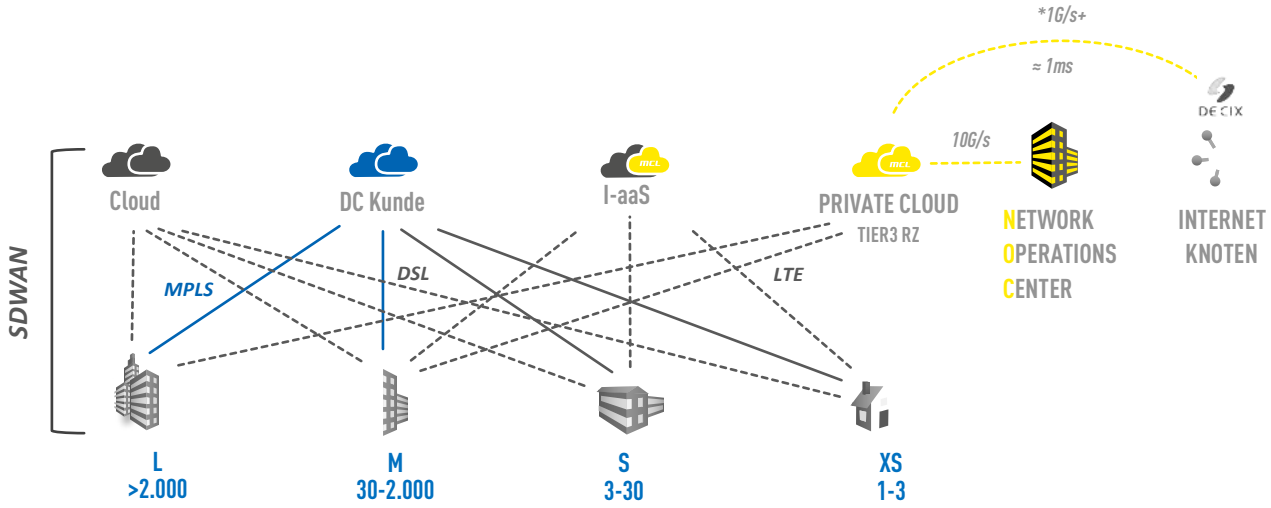
Secure Remote Access können Sie bei uns auch „as a Service“ beziehen.
Dahinter verbirgt sich eine Enterprise-Security-Lösung, die wir für Sie zusammengestellt haben: sicherer verschlüsselter Internetzugang, Client-Schutz gegen Malware und Phishing sowie sicheres Surfen. Das Herzstück ist eine Enterprise-Firewall, die DSGVO-konform innerhalb Deutschlands in der Cloud exklusiv für Sie gehostet wird. Diese skaliert beliebig, egal ob 50 oder 5.000 User. Die Installation der Client-Software auf dem mobilen Endgerät genügt, damit es für mobiles Arbeiten einsatzbereit ist.

Der Service kann auf **Monatsbasis pro Endgerät** bezogen werden, was Ihnen maximale Flexibilität gewährleistet. Damit wird nicht nur Ihre zentrale Firewall von komplexen, ressourcenfressenden Aufgaben entlastet, auch Ihre Internetanbindung wird nur mit dem Datenverkehr belegt, der wirklich in die Zentrale muss. Die Einbindung von Cloud-Diensten ist per Design vorgesehen.

OpenVPN / SSL-VPN / IPSEC sind weitere Software-Optionen, mit denen bestehende und zusätzliche Clients gegebenenfalls sogar mit Bordmitteln des Betriebssystems sicher ins Firmennetz gelangen. Wir prüfen für Sie, ob Ihre Infrastruktur die Anforderungen erfüllt, und machen uns auf Wunsch direkt an die Einrichtung von Router, Firewall und Clients.

„Ihre zentrale IT-Infrastruktur bzw. Ihre Ressourcen sind für den derzeitigen Bedarf nicht ausgelegt?“

MCL **Private Cloud** ist eine effiziente Möglichkeit, Dienste, Server und Speichersysteme schnell in ein Tier-3-Rechenzentrum umzuziehen oder dahin zu erweitern. Der Vorteil gegenüber großen Cloud-Anbietern liegt in der Individualität und strikten Separation der Hardware, sofern dies gewünscht ist. Eine eigene Firewall sowie
WAN-Anbindung runden das Angebot ab. Per Secure Remote Access können Sie selbst VMs verschieben oder die Speichersysteme konfigurieren. Damit erfüllt Private Cloud selbst KRITIS- Anforderungen, die weit über die Vorgaben der (EU-)DSGVO hinausgehen. Einen weiteren Vorteil stellt unsere räumliche Nähe zum Stuttgarter Internetknoten dar, der wiederum unmittelbar mit den datendurchsatzstärksten Internetkonten Europas in Frankfurt verbunden ist.



Mehr Speicher oder Compute Power – und was ist mit Ihrem Rechenzentrum?
Auf Nachfrage zahlreicher Kunden haben wir Bundles an Server- und Speichersystemen zusammengestellt, mit denen Sie Ihre VDI-Lösung einfach erweitern können, um kritische Kapazitätsgrenzen zu vermeiden. Denn bei einem kompletten Systemzusammenbruch durch Überlastung sind viele Mitarbeiter gleichzeitig betroffen und die Wiederherstellung der Arbeitsfähigkeit kann unter Umständen Stunden dauern, falls kein IT-Fachpersonal vor Ort ist.

4 MITTELFRISTIGE MASSNAHMEN

Wir alle hoffen auf eine Entspannung der momentanen Situation, doch auch verschärfte Vorgaben der Politik an die Wirtschaft können aktuelle Effekte auf die IT weiter verstärken. Mobilfunknetze und Provider kommen generell an Auslastungsgrenzen, so hatte beispielsweise im vergangenen Jahr Microsoft mit Ausfällen in der Azure-Cloud und in Diensten wie Office365 und Active Directory/DNS zu kämpfen. Kapazitätserweiterungen, Systemumstellung und Überprovisionierung könnten weitere Ausfälle zur Folge haben. Hybrid- Cloud-Lösungen mit neuster Architektur wie Docker verhalten sich in beiden Welten gleich und kombinieren die Vorteile.

4.1 Schutzbedarf nicht vernachlässigen.

Angriffe auf die IT-Infrastruktur werden in nächster Zeit voraussichtlich zunehmen. Machen Sie nicht voreilig Kompromisse bei den Sicherheitsanforderungen.
Eine ganze „Industrie“ lauert auf leichtes Spiel, um schlecht geschützte Clients zu kompromittieren und Schadsoftware zu installieren. Die Folgen wären unternehmerisch mindestens ebenso hart wie der Ausfall vieler Mitarbeiter selbst.

- Nehmen Sie den Nutzern die lokalen Adminrechte, um Angriffe durch Schadsoftware zu vermeiden.
- Sensibilisieren Sie Ihre Mitarbeiter per Video bzw. Konferenz für mögliche Angriffe im Kontext der aktuellen Situation. So könnten etwa Phishing-Mails dazu auffordern, Links der Firmen-IT zu öffnen, um wichtige Funktionen zu aktivieren. Fake-Firmen-Cloud-Share-Accounts werden möglicherweise mit Ihrem Firmennamen und echtem User-Namen versendet. Wer dann versucht, sich mit seinem AD-Login anzumelden oder auf das Attachment klickt, hat bereits verloren. Im Glauben, mit Kollegen zu kollaborieren, sind Nutzer versucht, sensible Firmendaten hochzuladen.
  Fordern Sie Ihre Kolleginnen und Kollegen auf, verdächtige E-Mails zu melden, sofern Sie nicht über eine integrierte Softwarelösung für manuelle Quarantäne im E-Mail Client verfügen.
- Vermutlich ist Ihr System aktuell in einem Ausmaß für Mitarbeiter von extern erreichbar wie nie zuvor. Schützen Sie es deshalb mit Backups gegen Ransomware und Datenverlust, selbst wenn Sie sich relativ sicher fühlen. Zusätzliche Server oder Cloud-Backups können das Risiko zusätzlich begrenzen.
- Bieten Sie ausreichende und praktische Möglichkeiten zum Datenaustausch, Ihre Mitarbeiter helfen sich sonst selbst mit Dropbox und Co. Auch das lokale Speichern von Daten birgt Gefahren. Nutzen Sie BIOS-Schutzmechanismen ebenso wie Festplattenverschlüsselung. Bei einem Diebstahl sind Sie erst dann gesetzlich verpflichtet, den Verlust personenbezogener Daten zu melden, wenn diese für Diebe lesbar (unverschlüsselt gespeichert) sind.

Noch weiter kann der Einsatz von MDM (Mobile Device Management) gehen. Damit können Sie beispielsweise Endgeräte orten und remote löschen. Das Löschen erfolgt idealerweise auch bei vielfacher Falscheingabe von Passwörtern automatisch.

- Schieben Sie Dokumentation, Notfallhandbuch und Risikomanagement nicht länger auf. Planen Sie Zeit und Budget, solange Sie dafür auf offene Ohren bei den Entscheidern stoßen. Sich professionelle externe Hilfe zu holen, zeugt vom besonnenen Umgang mit Ressourcen.

MCL unterstützt Sie gerne mit Tests zum Nutzerverhalten und dem zielgerichteten Training Ihrer Mitarbeiter. Unsere fingierten E-Mails prüfen die Wachsamkeit, ohne Schaden für Ihr Unternehmen anzurichten. Und unser **Factory Service** konfiguriert Ihre Systeme vorab entsprechend Ihrer Konzernrichtlinien.

4.2 Richtig mobil arbeiten

Sofern Sie keine bestehende Lösung ausbauen können, machen Sie sich über eine Collaboration-Lösung Gedanken. Diese erleichtert das effektive Arbeiten, Kommunizieren und Austauschen von Daten im Team, unabhängig vom Ort der Arbeit und mit einem hohen Maß an Sicherheit.

Mit einer kostenlosen Version von Teams können Sie bis zu einem Jahr chatten, Videoanrufe durchführen, bis zu 10 Gigabyte Daten in einer geschützten Cloud ablegen, Daten in Echtzeit teilen und gemeinsam an Dokumenten arbeiten.

5 LANGFRISTIGE MASSNAHMEN

Bereits heute ist klar, dass sich unsere Arbeitskultur schneller verändern wird als erwartet. Die hier vorgestellten Maßnahmen werden sicher über das Jahr 2020 und die aktuelle Krisensituation hinaus wirkungsvoll bleiben – selbst und gerade vor dem Hintergrund einer sich permanent verändernden IT-Welt.

5.1 Zukünftige Aspekte bei der IT-Planung

Viele der spontan beschafften mobilen Arbeitsplätze bleiben auch in Zukunft erhalten. Denn nicht nur die Generation der Millennials und noch jüngere Generationen werden darauf Wert legen, vielmehr wird der generelle Anspruch sein, sämtliche Daten- und Kommunikationsdienste von überall in gleicher Weise nutzen zu können.
In letzter Konsequenz sogar unabhängig vom Endgerät. Ob Smartphones in Kombination mit Maus, Monitor und Tastatur Notebooks verdrängen, die zuvor Desktops abgelöst haben, bleibt derzeit noch Spekulation. In vielen Fällen würde die Rechenleistung jedoch ausreichen. Bei sogenannten Convertibles verschmelzen Tablet und PC zu einem Gerät. Der Stift findet seine Renaissance. Die praktischen und kreatives Möglichkeiten machen sich vor allem Management und Marketing zunutze, trotz eines höheren Preises der Geräte.
Die private Nutzung des Firmengeräts wie das sichere Aufrufen von Firmen-Apps auf dem privaten Endgerät stehen selten auf der Wunschliste der IT-Abteilung, wohl aber auf der der Nutzer. Physikalische SIM-Karten werden durch Software (eSIM) entfallen, wenn sich die Provider nicht dagegen verwehren. Fachabteilungen stellen immer stärker restriktive IT-Vorgaben in Frage, sobald das Nutzererlebnis im täglichen Umgang negativ ausfällt. IoT-Geräte kommen hinzu, auch wenn sie nicht als solche berücksichtigt wurden. Insgesamt werden Systeme sicher nicht weniger komplex, aber die Orchestrierung kann mit der richtigen Strategie beschleunigt, automatisiert und vereinfacht werden.

5.2 Stichpunkte

- Prüfen Sie, welche Applikationen und Systeme Cloud-ready sind und langfristig in Ihrem Unternehmen bestehen werden. Setzen Sie sich mit Kubernetes und Docker auseinander, auch für Hybrid Cloud, oder On-Prem-Anwendungen. Verharren Sie nicht auf Virtualisierungslösungen, die technologisch gerade überholt werden.
- Sind Ihre Unternehmensanwendungen unabhängig vom Endgerät und Betriebssystem flexibel einsetzbar?
- Achten Sie auf aktuelle Funkstandards wie 5G und WiFi 6. Die billigsten Geräte haben meist die schlechtesten Treiber, was sich schnell rächen kann.
- Machen Sie regelmäßig einen Security Audit. Anfangs mit Vorher-Nachher-Check, später mit wechselnden Dienstleistern.
- Nutzen Sie Management- und Monitoring-Lösungen, die über APIs untereinander und mit Ihrer Sicherheitslösung kommunizieren können. Je weniger es in Summe sind, desto besser. Automatisierung, Flexibilität und hohe Transparenz sind wichtige Faktoren. KI- und Cloud-Features sollten für Sie einen klaren Mehrwert darstellen und nicht nur schicke Charts füttern. Die Historie sollte mindestens 30 Tage für Metadaten und 1 Jahr für Konfigurationsänderungen betragen.

5.3 Rolle der IT

Verstehen Sie Ihre IT-Abteilung als Selbermacher und Alleskönner, so wird es zunehmend schwieriger, den Anforderungen des Unternehmens in allen Bereichen dauerhaft gerecht zu werden. Suchen Sie sich wenige, starke Partner für Aufgaben, die in Eigenleistung zu langsam umsetzbar, weder wirtschaftlich noch attraktiv sind.
MCL unterhält Partnerschaften zu den wichtigsten IT-Herstellern am Markt und ist im hohen Maße als Unternehmen und mit unseren Spezialisten zertifiziert.

Versionskontrolle

2020.03.18-1	Version	Zuletzt geändert
18.03.2020	Datum	christian.priskel@mcl.de

Disclaimer

Dieses Dokument ist geschütztes Eigentum der Firma MCL Computer & Zubehör GmbH.
Ein verlinken von anderen Internetseiten, Portalen, Apps ist auch ohne Rückfrage mit einem Quellverweis gestattet. Auszüge und Zitate müssen als solche kenntlich gemacht werden und jeweils unmittelbar davor, oder danach lesbar selbigen Quellverweis *Quelle: MCL Computer & Zubehör / mcl.de* erhalten.

Das Speichern, Drucken und Weiterleiten zu nicht-kommerziellen Zwecken ist gestattet.
Jedwede sonstige Offenlegung, Vervielfältigung oder Verwendung des Dokuments, gleich ob im Ganzen oder in Teilen, erfordert die Freigabe durch MCL Computer & Zubehör GmbH.
Diese kann über unser Kontaktformular https://mcl.de/kontakt erfragt werden.

Jegliche enthaltenen Kommentare, Äußerungen, Auslegungen zu gesetzlichen Regelungen und geltendem Recht sind unverbindlich. Die Firma MCL Computer & Zubehör GmbH und deren Mitarbeiter erbringen keine Rechtsberatung.