cloud and more
consulting GmbH

IT SICHERHEIT CHECK

IT Sicherheit Analyse und wie Sie Ihre unternehmerischen Risiken minimieren können

cloud and more consulting GmbH

Adresse:
Melkergasse 12
A-2500 Baden, Österreich
www.cloudandmore.at

Telefon: +43(2252)890340
Fax: +43(2252)890340-15
office@cloudandmore.at

VORERST

VIELEN DANK

FÜR IHR INTERESSE !

Wir freuen uns sehr, Ihnen unser ePaper vorstellen zu können und so zu Ihrer IT Sicherheit beitragen zu dürfen. Als Anbieter von Komplettlösungen rund um IT Sicherheit, Wartung der IT Infrastruktur, Backup, Firewall, Software und Hardware Komponeneten werden wir oft von Kunden gefragt: "Wie erkenne ich eigentlich Bedrohungen", "Was ist der Unterschied zwischen malware und ransomware" oder "Was kann ich machen, wenn mein System infiziert wurde"?

Die brenennden Fragen und vor allem die Antworten inkl. Tipps haben wir in unserem ePaper zusammengefasst. Darüber hinaus legen wir gleich kleine Checklisten bei, anhand diesen können Sie leicht Ihren individuellen Status zu Ihrer IT Sicherheit prüfen, mit oder ohne unsere Begleitung. Viel Freude beim Lesen wünscht Ihnen

Mag. Wolfgang Lindorfer

Geschäftsführer

INHALT

1

EINLEITUNG

ZU IT SICHERHEIT UND WIE DAS UNTERNEHMERISCHE RISIKO MINIMIERT WERDEN KANN

DIE HERAUSFORDERUNG

Die Sicherheit, sagen Viele, ist ein subjektives Empfinden über die Risiken, die wir bereit sind, einzugehen. Das ist sehr individuell. Trotzdem gibt es Indikatoren, die dieses Empfinden eindeutig bestimmen können. Vor allem, wenn es um die Sicherheit unserer Daten und IT Systeme geht, um die Kontinuität unserer Betriebsprozesse und, genauer gesagt, um unsere geschäftliche Existenz.

In unserem ePaper „Risikoanalyse" fassen wir für Sie die wichtigsten Bereiche zusammen, und zeigen Ihnen Stellen auf, wo Ihre eigene IT Sicherheit überprüft und verbessert werden kann.

RISIKEN ERKENNEN UND VORBEUGEN

Mit unserer Risikoanalyse bekommen Sie einen Überblick über die wichtigsten Check-Points und die Auskunft darüber, wie anfällig oder nicht anfällig Ihr Unternehmen derzeit gegen den Befall z.B. eines erschlüsselungs-Trojaners ist, was Sie im Falle einer Cyberattacke tun müssen und wie schnell Sie zum normalen Tagesbetrieb zurückkehren können.

.

CHECK LISTEN

Praktische Tipps und kleine Helferleien in Form von Check-Listen finden Sie bei jedem Abschnitt. Sie helfen beim Erkennen, was überprüft werden soll, wie es Ihren Systemen geht, wo es eventuell noch Verbesserungspotenziale gibt und wie die Daten noch besser geschützt werden können. Sehr viel davon wissen wir bereits und die Lösungen liegen praktisch in unseren Händen und nicht nur an der Verantwortung der Technik. Sie hängen auch oft von unserer Sensibilisierung für dieses Thema ab und von unseren Verhaltensmustern beim täglichen Umgang mit E-Mails, Daten, Links, Datenschutzrichtlinien, etc...

BUSINESS KONTINUITÄT

Nicht jeder Hackerangriff oder Befall von Crypto Tojanern kann alleine mit der Änderung unserer Arbeitsroutinen und Standardisierungen verhindert werden, aber diese Zwischenfälle lassen sich damit deutlich reduzieren. Zu den Standards gehören IT Systeme, die die Infrastruktur ausreichend schützten (z.B. Firewall, Backups, Antispam-Antivirussoftware, Software Updates, Webfilter etc). Sie sind heutzutage einfach unerlässlich.
Sollte es trotz allen Maßnahmen einmal passieren und nach einem Befall Ihre Daten verschlüsselt sein, zeigen wir Ihnen auf und analysieren, wo die Ursache liegt und wie Sie Ihre Systeme und Daten in Zukunft noch besser schützen können. Bei Bedarf kann unter dem Aspekt der Wiederherstellbarkeit nach einem Problem auch Ihre Hardware analysiert werden um herauszufinden, ob Ihre wichtigsten Komponenten in Garantie sind, und am besten noch in ‚vor Ort' Garantie, damit auch im Falle eines Hardwaredefekts das Tagesgeschäft so schnell wie möglich wiederhergestellt werden kann.
Weitere Services für IT Sicherheit und IT Kontinuität aus unserem Portfolio finden Sie bei Interesse auf unserer Website unter: Link.

VIERENFILTER INKL. DER ÜBERPRÜFUNG DER ANHAENGE UND LINKS

Sind meine Systeme in der Lage, Schadsoftware zu erkennen, bevor sie in das Herz des Unternehmens galangen. Werden alle Anhäge und Links in E-Mails überprüft und verdächtige Dateien oder Links rechtzeitig ausgefiltert?

SPAMFILTER

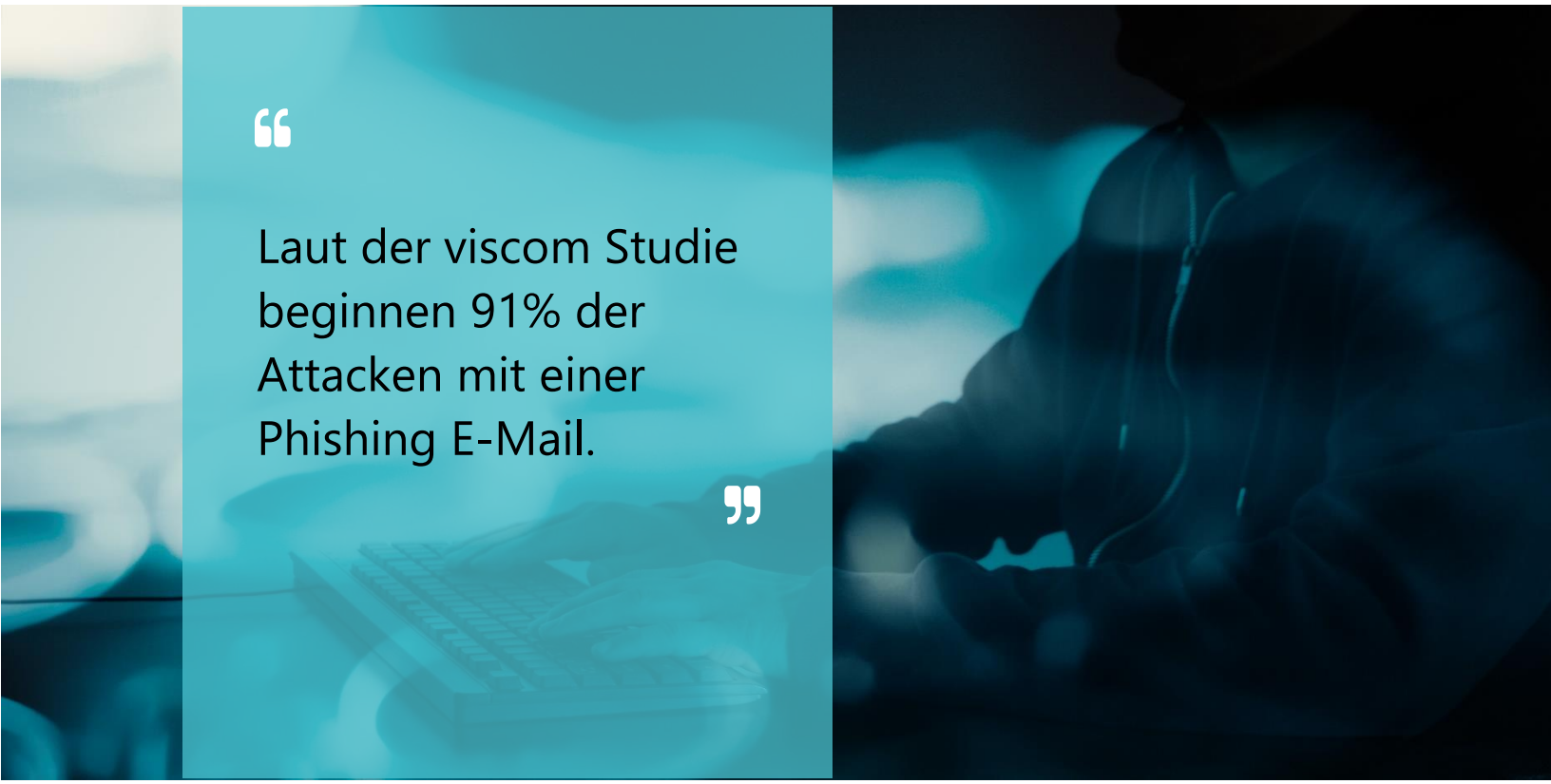
Stammen die E-Mails, die in meinem Postfach landen, von vertrauenswürdigen Adressen oder von mir bekannten Personen? Kommt Ihnen eine E-Mail verdächtigt vor und beinhaltet vielleicht auch grammatikalische Fehler? Finger weg!

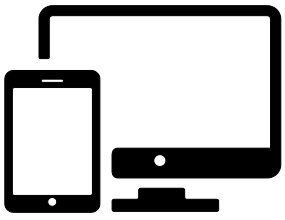
… ZU ÜBERPRÜFENDE

SYSTEME UND KOMPONENTEN

DER TAGTÄGLICHE RISIKOFAKTOR

2 E-MAIL





Im Jahr 2016 passierten 4.000 Milliarden Attacken durch Schadsoftware … und das an einem Tag.

Viele davon hätten aber verhindert werden können.

SCHADSOFTWARE UND VERSCHLÜSSELUNGSTROJANER

WannaCry, Red Petya und Goldeneye sind die originell klingenden Namen für eine Schadsoftware, die nicht nur den Unfung auf unseren PC treiben, sondern unsere Daten stehlen und / oder verschlüsseln. Die moderne digitale Kriminalität boomt und bringt Lösegelder in Miliardenhöhe. Das Ziel der Attaken sind inzwischen Firmen oder Behörden, die mit der Veröffentlichung der sensiblen Daten bedroht werden. Auch Privatpersonen bleiben nicht länger verschont und werden erpresst, von Daten und Geld beraubt.

Umso wichtiger werden der Schutz und die Fähigkeit, diese Bedrohungen zu erkennen.

Der häufigste Einfallsweg eines Verschlüsselungstrojaners ist über eine E-Mail, sei es über das Öffnen eines Dateianhangs oder das Anklicken eines Hyperlinks. Deswegen ist es von höchster Wichtigkeit, dass Ihr E-Mail System bestens geschützt ist um nahezu ausschließen zu können, dass solche verseuchten E-Mails bis zu Ihrem E-Mail Clientprogramm gelangen

VerschlüsselungsTROJANER

Krypto / - Erpressungstrojaner, häufig auch als ransomware genannt sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Dabei werden private Daten auf dem fremden Computer verschlüsselt oder der Zugriff auf sie verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern.

DER RICHTIGE UMGANG MIT E-MAILS

Der Umgang mit E-Mails ist auf dem ersten Blick nicht schwer. Aber gerade durch die Einfachheit und Beliebtheit der E-Mail, geht von Ihr auch ein hohes Risiko aus. Internetkriminelle nutzen E-Mails um Computerviren zu verteilen, Spam-Mails zu versenden und um Leser mit sog. Phishing-Methoden in die Falle zu locken.

Aktuell findet man viel Schadcode in E-Mails die vorgeben, Rechnungen zu beinhalten. Diese werden im Word Format (.doc) zugesendet und nicht im Adobe Reader (.pdf) Format, alleine das ist schon verdächtig, weil für Rechnungen eigentlich nicht zulässig.
Weitere beliebte Aufhänger, die den Benutzer zum Klicken bringen sollen, sind Zustellberichte von Paketdiensten und diverse Informationen von Banken und Bezahldiensten.

> “Die Verbreitung der Verschlüsselungs-trojaner stieg im Jahr 2016 um 6000% — und kostete Firmen $1Mld.”

DAS RICHTIGE VERHALTEN

Grundsätzlich kann man sich mit folgenden Schritten recht effektiv vor falschen Klicks schützen:

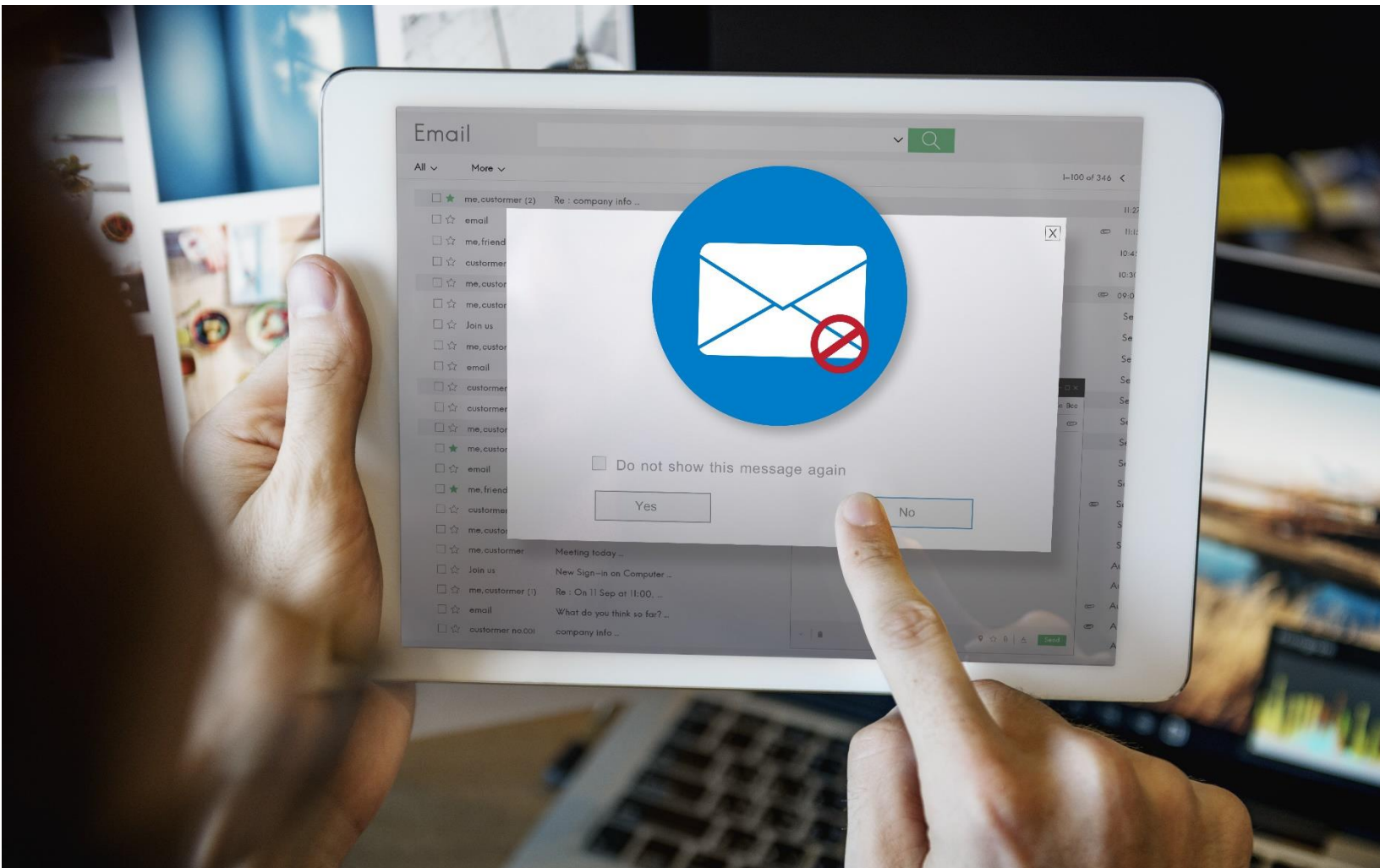
- Klicken Sie nicht neben anderen Tätigkeiten wie telefonieren neu ankommende E-Mails an, **konzentrieren** Sie sich darauf, was Sie anklicken.
- Öffnen Sie keine **Anhänge** aus E-Mails, denen Sie nicht 100%ig vertrauen. Auch Anhänge, die aussehen, als wären Sie ein Bild oder eine einfache Textdatei, können gefährlich sein. Computerkriminelle nennen eine infizierte Datei z.B. „deinfoto.jpg.exe“. Je nach Ordner-Einstellung wird Windows bekannte Dateiendungen (hier .exe) ausblenden. Somit sieht es für Sie aus, als hieße die Datei „deinfoto.jpg“. Während unbedarfte Internetnutzer annehmen, es handle sich um ein einfaches Bild, wird beim Anklicken eine Anwendung gestartet, die den Virus oder den Wurm in Ihrem System verteilt.

- Werfen Sie einen Blick auf den **Absender** und den **Betreff**. Wenn Sie E-Mails erhalten, bei denen Sie bereits am Absender und Betreff ahnen, dass es sich um eine Spam-Mail oder eine E-Mail handelt, die nicht seriös und vertrauenswürdig ist, sollten Sie diese erst gar nicht öffnen.

- Anklicken von **Links**. Ähnliche wie beim Öffnen von Anhängen, kann auch das Anklicken eines Links ein Sicherheitsrisiko darstellen. So könnte die Zielseite Schadroutinen enthalten, die sich auf ein ungeschütztes System leicht übertragen können. Klicken Sie deshalb nur Links in E-Mails an, wenn Sie dem Sender der E-Mail trauen.

- Vertrauen in den **Absender**. Der Absender, den Ihnen Ihr E-Mail-Programm anzeigt, muss nicht zwangsläufig der echte Absender sein. Es ist technisch keine sonderlich große Herausforderung, den Absender einer E-Mail zu fälschen. Wenn Ihnen also Ihr Arbeitskollege auf einmal seltsame E-Mails schreibt, sollten Sie hellhörig und vorsichtig werden!

- Oft kann man an einem Link sehr gut erkennen, dass er zu einem falschen Ziel führt indem man einfach mit der Maus darüberfährt aber natürlich nicht klickt. Hier ein paar Beispiele:



Sehr geehrter Kunde,

Wir sind derzeit die Aktualisierung unserer Datenbank und alle Netbanking-Konten müssen aktualisiert und aktiviert werden, um weiterhin diesen Vorteil zu nutzen, bitten wir Sie Ihre Daten in den folgenden Link, um zu bestätigen:

http://247discountshop.com/admin/estatspark/index.htm
Klicken, um Link zu folgen

Erste-Sparkasse Netbanking Aktualisierung: Klicken Sie hier

Dank für Ihre Mitarbeit und Verständnis.

Mit freundlichen Grüßen.
Ihr Erste-Sparkasse Kunden service.

Sehr geehrte Kunden,

Erste Bank, Wir möchten Sie darauf hinweisen, die Zugang zu Ihrem Online-Banking wird daher vorübergehend eingeschränkt. Komplett neu erstellen Ihr Konto und uneingeschränkten Zugang haben, bestätigen Sie bitte d

http://forumenfermagememacao.com.br/estatspark/index.htm
Klicken, um Link zu folgen

alisieren:

Erste-Sparkasse NetBanking-Aktualisierung: klicken Sie hier

Nachdem ein Mitarbeiter unserer Bank Ihre Daten überprüft hat, ist Ihr online-banking wieder zur Gänze hergestellt.

Vielen Dank für Ihre Mitarbeit!

Mit freundlichen Grüßen,
Ihr Erste-Sparkasse Kunden service.

Malware (Schadprogramm)

Als Malware werden alle Programme bezeichnet, die dazu entwickelt wurden, Benutzern Schaden zuzufügen. Es gibt zahlreiche Unterarten von Malware - zum Beispiel Viren, Trojaner, Rootkits oder Spyware. Alle arbeiten anders und haben verschiedene Aufgaben. Ein Ziel haben Sie jedoch gemein: Ihnen zu schaden.

DIE BANKEN UND DIE STELLUNGNAHMEN

Auf den eigenen Seiten der Hausbank findet man auch immer aktuelle Infos zu diesen Themen, auch hierzu ein Muster inkl. Erklärung:

„Derzeit versuchen Betrüger von Kunden Zugangsdaten zum Digitalen Banking zu erschleichen.
Mittels Phishing-Mails werden Kunden auf gefälschte Seiten gelockt wo sie Daten eingeben sollen.
Als Vorwand dient die Information eines wichtigen Sicherheitsupdates.
Dabei wird mitgeteilt, dass das Konto gesperrt wurde und das Sicherheitsupdate durchzuführen sei.
Ebenso werden weitere Maßnahmen am Konto angedroht, wenn dies nicht binnen 14 Tagen erfolgt.
Zusätzlich würde noch Bearbeitungsgebühr anfallen. Derzeit werden diese mit 69,95 EUR kommuniziert.
Dabei handelt es sich dann natürlich NICHT um ein Mail der Hausbank.
Ihr Konto wurde deshalb nicht gesperrt; es ist kein Sicherheitsupdate notwendig!
Bitte folgen Sie daher keinesfalls den Anweisungen
• Weder am Computer noch im Falle eines Anrufes unbekannter Personen im Namen der Hausbank
• Klicken Sie keine Links in dem gefälschten E-Mail und öffnen Sie in der Folge keine Dateien
Wenn Sie Daten bekanntgegeben haben oder bei Fragen wenden Sie sich bitte an die den Support der Hausbank.
Wir sind selbstverständlich jederzeit gerne für Sie da!“

CHECK LISTE

And we can do more!

PHISHING E-MAILS

Phishing Mails haben ein Ziel, an Ihr Geld zu kommen. Mittels dieser Nachrichten werden persönliche Daten wie Kennwörte oder Bankkonto Informationen über Links zu verdächtigen Websiten versucht zu bekommen. Geben Sie niemals diese geforderten Informationen weiter.

SPAM E-MAILS

Bekommen Sie viele unerwünschte Werbenachrichten per E-Mail? Dann haben Sie wahrscheinlich keinen Spamfilter im Einsatz. Ein Spamfilter verschiebt verdächtige E-Mails in einen separaten Spam-Ordner oder löscht diese, wenn es ganz eindeutigt Spam Nachrichten sind.

In den nächsten Kapiteln werden wir uns mit der Technik auseinandersetzen, die bei Sicherheitsfragen die nötige Unterstützung bietet. Dazu zählen z.B. Backup Routinen, Hardwarekomponenten, Diverse Filtermöglichkeiten, Monitoring und Alerting, der richtige Umgang mit den Daten und Systemen und noch so vieles mehr.

Die beste Technik wird jedoch keinen 100%igen Schutz bieten können, deswegen ist der umsichtige Umgang mit z.B. E-Mails extrem wichtig.

ENDPOINT SECURITY

CISCO STUDIE

Laut dieser Studie erachten 65% der Unternehmen die Nachlässigkeit bei eigenen Mitarbeitern als die zweitgröste Bedrohung. Cyberangriff ist auf Platz 1.

Seitdem das iPhone auf den Markt gebracht wurde, tragen wir mindestens 2 Geräte mit uns – obligatorisch das Smartphone und zusätzlich den z.B. Laptop. Später ist auch noch das Tablet dazugekommen. Das stellt die Unternehmen vor neue Herausforderungen, die das Unternehmen nicht immer selbst beeinflussen kann, es trägt aber die Verantwortung für die Sicherheit der Unternehmensdaten und der Systeme. Denn die ständig wachsende Anzahl der Geräte erhöht das Risiko des Datenklaus oder des Ausspähens oder gar Angriffs. Die Realität zeigt, dass gerade die mobilen Geräte (Endpoints/Endpunkte) nicht ausreichend geschützt werden, dabei sind sie ein Tor in das eigene Firmennetzwerk und werden dadurch oft zu einem Angriffspunkt.

3

ENDPOINT SECURITY

SIND DIE SMARTPHONES IHRER MITARBEITER AUSREICHEND GESCHÜTZT?

DIE HERAUSFORDERUNG

Die Angriffstaktiken werden immer intelligenter und ausgeklügelter. Der Schutz soll diesen Strategien in Nichts nachstehen, würde man meinen. Eine IDG Studie belegt aber, dass nur die Hälfte der Unternehmen einen proaktiven Ansatz verfolgt, was der Schutz der Endpunkte betrifft.

Früher haben Unternehmen einen reaktiven Ansatz „prevent und protect"verfolgt. Das war man ausreichend. Heute ist eine kontinuierliche Überwachung gefragt, wo alle Auffälligkeiten rechtzeitig erkannt werden. Der Ansatz „detect and respond" ist der neue Standard.

DER SCHUTZ

- Der Schutz der Endpunkte beginnt mit der akribischen Aufzeichnung aller Geräte und aller Security Maßnahmen, die getroffen werden. Erst dann gibt's es eine Basisinformation, anhand derer festgestellt werden kann, welche Sicherheitslücken ev. vorhanden sind und wie diese geschlossen werden können.
  Wichtig dabei ist, alle Schutzvorkehrungen mit dem aktiven Monitoring der Geräte zu kombinieren um die möglichen Auffälligkeiten rechtzeitig mitzubekommen.

- Der richtige Umgang mit den Geräten ist ein ebenfalls ein wichtiger Faktor, der erwähnt werden muss. Eine bewusste Verwendung des Smartphones oder Laptops sowie sichere Passwörter gehören zu den absoluten Basic Security Maßnahmen.

- Immer aktuelle Software einsetzen, da ältere Versionen Sicherheitslücken aufweisen könnten. Die Software soll immer aus vertrauensnwürdigen Quellen oder Website stammen.

Richtlinie für ein sicheres Passwort:

Ein Passwort soll enthalten:

- Mindesten 8-10 Zeichen
- Klein- und Großbuchstaben
- Zahlen und Sonderzeichen

Ein Passwort darf **nicht** enthalten:

- Worte, die in einem Wörterbuch vorkommen
- Geburtsdatum, Namen oder Kennzeichen
- Vorher verwendete Passwörtre
- Woanders verwendete Passwörter

Außerdem:
Notieren Sie das Passwort nicht!
Nutzen Sie keine kostenfreien Passwort Safes!
Ändern Sie Passwörter nach 30 Tagen oder immer beim Verdacht auf Kenntnissnahme durch Dritte!

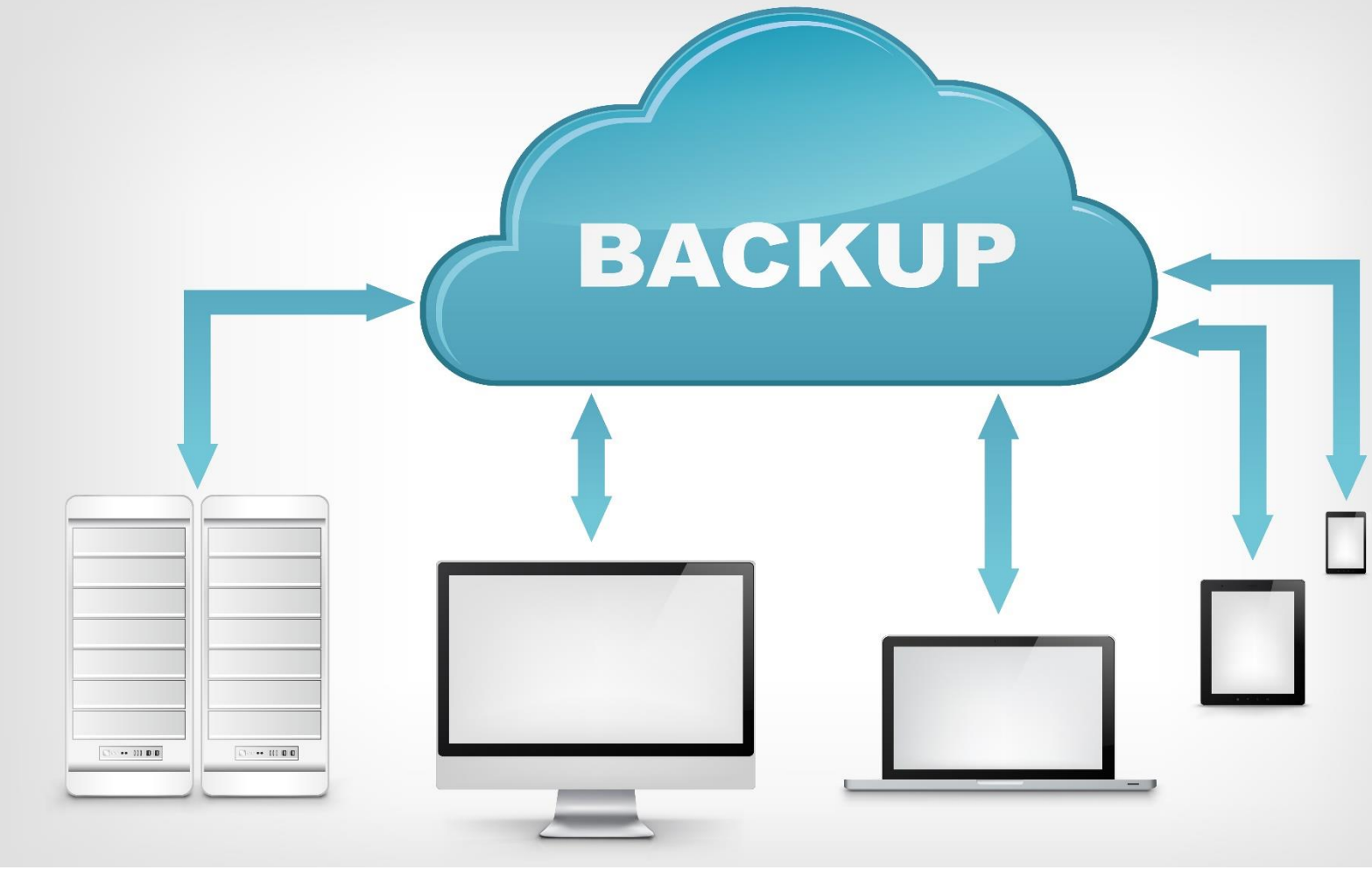
4

BACKUP SYSTEME UND ROUTINEN

... SCHÜTZEN SIE SICH VOR DATENVERLUSTEN

EIN BACKUP MINIMIERT DAS VERLUSTRISIKO

Schützen Sie ausreichend Ihre Daten und die Daten Ihrer Kunden?
Oder gehen Sie dabei vermeintliche Risiken ein?



3 – 2 – 1 – 0 REGEL

Sollte einmal, trotz aller Vorkehrungen, ein Verschlüsselungstrojaner Ihren Datenbestand verschlüsseln, so ist es extrem wichtig, dass ihre Daten schnell und zuverlässig wiederhergestellt werden können, ohne Lösegeld zu zahlen.

Die 3-2-1-0 Regel schlägt vor, 3 unabhängige Kopien der Daten zu haben, den Einsatz von mindestens 2 unterschiedlichen Backup Medienarten (Festplatten, Bänder, online), mindestens 1 ausgelagertes Backup (zweiter Standort, online) um hoffentlich 0 Probleme bei der Wiederherstellung zu haben.

Ganz gefährlich sind ausschließliche Sicherungen auf nur ein Medium (eine USB Platte) und direkt verbundenen Medien, die bei einem Befall gleich mitbefallen werden können. Da sehr viele Unternehmen keinen zweiten Standort zur Verfügung haben, bieten sich bequeme online Sicherungsvarianten als Ergänzung an. Wichtig ist auch in diesem Zusammenhang, dass die Benutzer nicht auf alle Daten des Unternehmens zugreifen können, sondern nur auf die Daten, die für ihre tägliche Arbeit notwendig sind, damit im Falle des Falles nur ein gewisser Datenbestand angegriffen werden kann. Zusätzlich sollten so wenig Laufwerke wie möglich, sprich Netzwerklaufwerke, präsentiert werden, um die Ressourcen im Netzwerk hier auch relativ einfach schützen zu können. Denn keine Zugriffsmöglichkeit bedeutet im Normalfall auch keine Verschlüsselungsmöglichkeit. Weiters ist auch interessant in welchem Kontext gearbeitet wird, d.h. Personen sollten als normale Benutzer (Standardrechte) und nicht mit administrativen Rechten arbeiten. Weiters soll auch die eingesetzte Sicherungssoftware nicht in einem Administrator Kontext laufen, sondern mit einem eigenen für das Backup zur Verfügung gestellten Benutzer.

DER FAKTOR MENSCH

Was sehr oft vergessen wird, ist der Faktor Mensch. Er spielt immer die Schlüsselrolle beim Halten die Systeme up and running und beim sicheren Aufbewahren und Umgang mit den Daten, Laptops, Smartphones, etc. Daher es ist immens wichtig, die eigenen Mitarbeiter zu informieren und zu schulen über die Relevanz des richtigen Verhaltens.

SICHERUNGSSTRATEGIE

Unabhängig von der Größe des Unternehmens, empfielt sich jedenfalls eine Sicherungsstrategie zu haben. Sie sollte folgende Punkte beinhalten:

- mit welchen Datenklassen habe ich in meinem Geschäft zu tun denn
- Wichtige Unternehmensdaten sollen öfters gespeichert werden
- wo werden diese Daten gespeichert (optimal ist es, wenn sie auf einem zentralen Server liegen)
- wurden allen Daten in meinem Backup Konzept berücksichtigt? Welche Daten, wo, wie oft und wohin gesichert werden?
- sind meine Speicherorte abgetrennt, damit im Falle vom Befall von Crypro-Trojaner nicht alle Orte gleich verschlüsselt werden
- wie und wo werden Daten gesichert, die auf mobilen Geräten liegen

BACKUP IN DER CLOUD

Die letzte Frage hat eine einfache Antwort und gleich eine Alternative, die besonders für kleinere und mittlere Unternehmen interessant ist, nämlich die Cloud. Ein Backup in der Cloud ist für jedes Gerät und überall durchfühtbar. Die einzige Voraussetzung ist eine Internetverbindung. Für diese Art der Datensicherung wird keine weitere Infrastruktur benötigt und für die Wartung fallen auch keine Aufwände an. Bei dieser Alternative ist zu beachten, dass das Rechenzentrum nach Möglichkeit in Europa angesiedelt ist und darüber hinaus ist zu beachten, dass die Daten verschlüsselt transportiert und abgelegt werden und das das Rechenzentrum, wenn möglich, zertifiziert ist (z.B. ISO 27001).

CHECK LISTE

And we can do more!

ZU SCHÜTZENDE DATEN UND SYSTEME

Sie wissen den Status über die wichtigen Aspekte hier: welche Daten muss ich unbedingt schützen, aufgrund der gesetzlichen Auflagen z.B. EU-DSGVO und welche Daten sind für mein Unternehmen existenziell wichtig. Und welche Risiken gehe ich ein, wenn ich das nicht tue.

3 – 2 – 1 – 0 REGEL

Wie überprüfe ich die eigene Backup Strategie nach 3-2-1-0 Regel? Was ist für die Kontinuität der Geschäftsprozesse im Falle eines Ausfalls einiger Kernsysteme erforderlich?

NETZWERKLAUFWERKE UND LAUFWERKBUCHSTABEN

Welche Laufwerke werden den Usern präsentiert und welche sind nur dem Administrator vorbehalten? Wie viele Laufwerke sind empfehlenswert für meine IT Struktur?

AKTUELLE BACKUP LÖSUNG

Gibt es Backup Routinen in meinem Unternehmen? Bin ich in der Lage, im Falle eines Hacker Angriffs innerhalb der kürzesten Zeit, weiter zu arbeiten. Wo und wie oft werden Backups erstellt?

FREIGABEN UND RECHTEVERGABE

Wer hat Zugang zu welchen Daten und Systemen in meinem Unternehmen? Wie kann ich das Datenverlustrisiko mit einer angepassten Rechtevergabe limitieren?

ARBEITEN ALS BENUTZER ODER ADMINISTRATOR

Was muss ich beachten, wenn Personen mit unterschiedlichen Rollen auf bestimmte Daten zugreifen (Administrator, Bennutzer mit Lese- oder Vollzugriff)?

RTO UND RPO

Haben Sie Werte RTO (Recovery Time Objective) und RPO (Recovery Point Objective) festgelegt? Vereinfacht gesagt wie lange darf ein Restore dauern und wie aktuell sollen die Backup Daten sein.

ERGEBNISE UND VORSCHLÄGE

Un wenn Sie Unterstützung bei Analyse Ihrer Check Liste in Anspruch nehmen möchten, bieten wir Ihnen eine Unterstützung unserer Experten und führen eine komplette Analyse mit Ihnen durch.

RESTORETESTS

Um zu wissen, ob alles funktionieren wird, wenn es zu einem Problem kommt, müssen wir nicht bis zu einem Ernstfall warten. Dazu gibt es entsprechende Tests, die das belegen können, und das Risiko eines Verlustes weiter minimieren.

> **93% SECURITY MANAGERS SIND ÜBERFORDERT**
>
> Quelle: McAfee
>
> Die meisten IT-Sicherheitsabteilungen sind überfordert und nicht in der Lage, die Bedrohungen zu selektieren, sowie das Risiko richtig einzuschätzen.

5

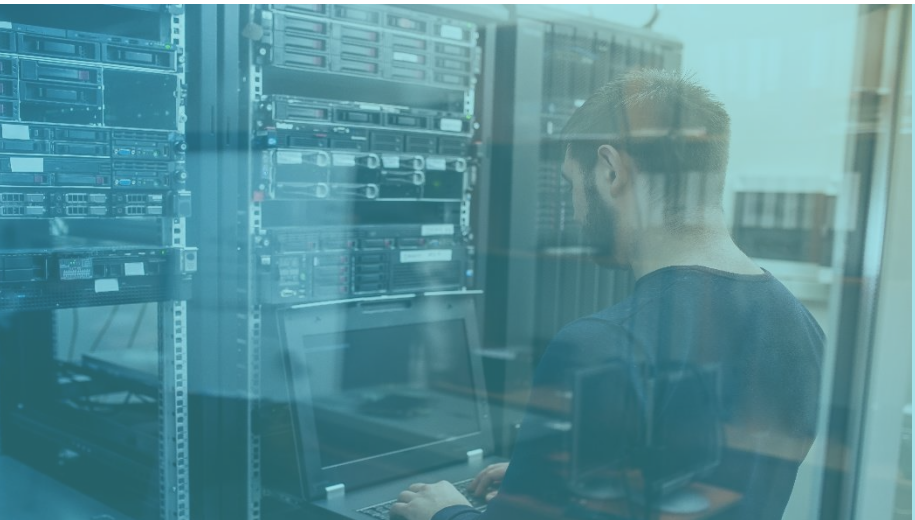
HARDWARE FÜR IHRE IT SICHERHEIT

Die wichtigsten Hardwarekomponenten und ihr Garantiestatus

Erst eine leistungsstarke IT Infrastruktur bildet die Basis für die entsprechende Sicherheit Ihrer Daten und Geschäftsprozesse.

DIE HARDWARE

Soll ein Sicherheitskonzept fehlerfrei funktionieren, verlangt es eine professionelle IT Infrastruktur. Sie muss alle Funktionen und IT Komponente untertstützen, die, am besten bereits bei der Planung, berücksichtigt wurden. Hierbei ist es wichtig, dass die Komponenten überhaupt noch in Garantie sind aber auch, dass es eine vor Ort Garantie gibt. Es macht bei den wichtigen Systemen keinen Sinn, wenn zum Beispiel zum Austauschen einer defekten Festplatte, diese eingesendet werden muss, fünf Tage unterwegs ist, vom Hersteller überprüft wird, ausgetauscht wird, zurückgesendet wird und das Zurücksenden weitere fünf Tage dauert.



Denn das würde im Endeffekt bedeuten, dass trotz Garantie das System zehn Tage lang ungeschützt wäre und bei einem weiteren Ausfall einer Festplatte eventuell einen Komplettausfall nach sich ziehen würde. Eine Hardwarelandschaft umfasst meistens passive und aktive Komponenten. Alle Aktiven brauchen eine Stromversorgung.

Damit auch das Netzwerk reibungslos funktioniert sollte es redundant ausgelegt sein oder zumindest die Möglichkeit bieten, nach einem Ausfall einer Komponente gleich ein Ersatzteil oder Übergangssystem bereit gestellt zu bekommen. Intern oder auch vom EDV Partner Ihres Vertrauens.

CHECK LISTE

And we can do more!

SPEICHERSYSTEME

Die Auswahl eines Speichersystems soll an die Datenmenge, Zugriffszeit und Verfügbarkeit der Daten angepasst werden. Es kann, je nach Anforderung, zwischen lokalen Festplattensystemen, Bandlaufwerken oder Cloud Speicher entschieden werden.

BACKUP SYSTEME

Backup Systeme dienen dazu, im Falle eines Datenverlustes, den gesamten Datenbestand wiederherzustellen. Ein Backupkonzept soll eher als ein Prozess gesehen werden, der immer wieder revidiert, getestet und angepasst wird.

FIREWALLS

Eine Firewall ist die erste Barierre zum Internet und regelt, welcher Datenverkehr in das interne Netzwerk durchdringen darf aber auch welcher nach außen gehen darf. Sie kann aber auch eine Eingangtor für Angriffe sein, wenn sie Sicherheitslücken aufweist. Die Firewallregeln sollten auf alle Fälle sorgfältig definiert werden.

NETZWERKKOMPONENTEN

Ein Netzwerk besteht in der Regel aus vielen Elementen. Beginnend von Kabel, Panelen, Dosen über Router und Switches bis zur Firewall. Die Komponenten sollen im IT Infrastruktur Konzept sorgfällting geplant und aufeinander abgestimmt werden.

6

IT MONITORING UND ALERTING

…. Das Ziel ist es, potentielle Probleme und Bedrohungen vorzusehen und zu beseitigen, bevor sie bemerkbar werden.

Monitoringsysteme liefern wichtige Informationen. Anhand solcher Daten können Fehler identifiziert und in Zukunft vermieden werden. Bei den IT Systemen machen sich manche Fehler nicht immer gleich bemerkbar. Nach längerem Zuwarten werden die Schäden immer größer verursachen und im Extremfall einen Totalausfall der Infrastruktur oder eines Teiles davon. Gerade beim Backup und beim Hardwarestatus ist es unerlässlich, dass tagesaktuelle Informationen vorliegen, ob die Sicherungen auch sauber durchgelaufen sind und ob die Hardware ordnungsgemäß funktioniert.

Es nützt die beste Hardwaregarantie nichts, wenn man nicht mitbekommt, wenn ein Teil getauscht werden müsste und jeder weitere Defekt das System komplett lahmlegen würde. Im Falle der Datensicherung verhält es sich genauso. Die beste Backup Software kann von Zeit zu Zeit Fehler bringen, die ein Eingreifen erfordern. Deswegen ist es auch hier unerlässlich immer zu wissen ob die Sicherungsjobs sauber laufen und keine Fehler

> Im Jahr 2016 haben die Organisationen weltweit $73,7 Mrd. Für Cybersecurity ausgegeben. Das ist ein Anstieg um 38% im Vergleich zum Vorjahr.
>
> Quelle: Fortune

UND WENN ES DARAUF ANKOMMT

Was macht einen guten IT Service so begehrenswert? Das Gefühl, beruhigt zu sein, wenn man einen richtigen und zuverlässigen Partner an der Seite weiß. Und ein besonderes Service zeichnet aus, dass sogar im Falle eines Ernstfalles auch die benötigten Ersatzteile zeitnah bereitgestellt werden und die Zeiten des Stillstandes und das eventuelle Risiko des Umsatzverlustes reduziert werden.

CHECK LISTE

And we can do more!

STATUS MONITORING

Das oberste Ziel des Monnitoring ist das Erkennen der potenziellen Probleme aus Tendenzen in historischen und aktuellen Daten. Diese Daten liefern aussagekräftige Informationen, die für die Muster für künftige Probleme eine Rolle spielen können. Auf diese Weise lassen sich viele Fehler gar vermeiden, bevor sie überhaupt entstehen oder bemerkt werden. Wissen Sie, wie es Ihren IT Systemen geht?

ALERTING

Damit keine größeren Schäden entstehen, muss über Ereignisse und Fehlverhalten in der IT Landschaft sofort informiert werden. Je nach Ernstfall und Vereinbarung soll ein SMS, E-Mail oder Alert auf einen dashboard abgesetzt werden. In vielen Fällen lassen sich damit teure Reparaturen oder Datenverluste vermeiden und die Verfügbarkeit der Systeme deutlich steigern. Werden Sie proaktiv benachrichtigt, falls notwendig?

AUCH FÜR KLEINERE BUDGETS

… gibt es gute Lösungen

In vielen Fällen ist es möglich, mit geringem finanziellen Einsatz, durch das Anmieten von Ressourcen in einem Rechenzentrum, sei es bei einem klassischen Provider oder einem Cloud Provider, die Gesamtlösung um ein Vielfaches zu verbessern. Das haben wir bei der online Sicherung schon kurz angesprochen aber auch Monitoring und Alerting oder Sicherheitslösungen, die in der Cloud, oder einem klassischen Rechenzentrum betrieben werden, und Sie dadurch keine eigenen Serversysteme vorhalten müssen, können enormes Einsparungspotenzial bei gleichzeitiger Steigerung der Sicherheit bringen. Auch ein direktes Speichern in einem Rechenzentrum bringt evntuell mehr Möglichkeiten und dadurch auch eine bessere Datensicherheit. Die ist z.B. ganz leicht durch den Mechanismus der Versionierung zu erzielen. D.h. es wird nicht nur immer die aktuelle Version einer Datei aufbehalten, sondern auch Vorgängerversionen, auf die man im Falle des Falles zurückgreifen kann. Zu solchen Fällen zählt nicht nur eine verschlüsselte Datei, sondern zum Beispiel auch eine überschriebene Datei, die ganz leicht durch den Benutzer selbst in eine altere Version zurückversetzt werden kann.

… KOSTENGÜNSTIGE

6 ERGÄNZUNGEN UND ABSICHERUNGEN

7 WIR

... CLOUD AND MORE CONSULTING GMBH

NICHT NUR CLOUD...

"Wir sind ein Team von begeisterten IT Experten und Beführworter der Cloud Technologie, überall wo es Sinn macht."

cloud and more consulting GmbH ist der zuverlässige Partner und ein Komplettanbieter, wenn es um die Planung, Betreuung und Optimierung der gesamten EDV Landschaft geht. Unsere Schwerpunkte sind die Planung, Implementierung und das Service von Infrastruktur-, Sicherheits- und Kommunikationslösungen von Klein- und Mittelbetrieben sowie Schulen.

LOKALER PARTNER

Ein zuverlässiger Partner in Ihrer Nähe in Wien, Niederösterreich und in Burgenland.

BESTE TECHNOLOGIE

Kooperationen mit vielen renomierten Herstellern wie Microsoft, Fortinet, Veeam, Ubiquity, Dell, Fujitsu.

KOMPLETTLÖSUNGEN

Komplettanbieter für traditionelle, cloud basierte und hybride Kommunikations-, Sicherheits- und Inftrstrukturlösungen

UNSERE EMPFEHLUNG

8 | WARTUNG

FÜR JEDE GRÖßE UND ANFORDERUNG

FÜHRENDE TECHNOLOGIE

SCHNELL IN IHRER NÄHE

INDIVIDUELLE SLA

Besonders Klein- und Mittelbetriebe sowie alle Unternehmen, die keine eigene IT Abteilung haben, müssen sich in der Regel auch um die IT Basis kümmern, den Mitarbeitern alle nötigen Systeme bereit stellen und sicherstellen, dass auch alle gesetzlichen Anforderungen (Datenschutz, Aufbewahrungspflichte etc…), erfüllt sind.

Nicht selten werden dabei hohe interne Kosten in Kauf genommen. Daher ist es eine gute und im Vergleich eine günstige Alternative, einen zuverlässigen Partner Ihres Vertrauens für fachgerechte Betreuung Ihrer gesamten IT Infrastruktur, oder deren Teile, zu wissen. Er sollte auf Ihre Bedürfnisse eingehen können, möglichst Hersteller-unabhängig agieren, in Ihrer Nähe oder schnell verfügbar sein. Bei Gelegenheit schauen Sie gerne auf unsere Webseite um Details zu unseren Dienstleistungspaketen für Managed Backup, Managed Workstation oder Managed Office Kommunikation für ein sicheres und störungfreies Arbeiten zu erfahren.

CLOUD AND MORE CONSULTING GMBH

Firmensitz:
Melkergasse 12
A-2500 Baden
Telefon: +43(2252)890340
Fax: +43(2252)890340-15
E-Mail: office@cloudandmore.at
Web: www. cloudandmore.at

Office:
Brown-Boveri Straße 8/1/5
A-2351, Wr. Neudorf
Telefon: +43(2252)890340
Fax: +43(2252)890340-15
E-Mail: office@cloudandmore.at
Web: www. cloudandmore.at

VIELEN DANK

FÜR DOWLNOAD