

Dieses Dokument adressiert Geschäftsleitungen und Eigentümer von kleinen und mittelständischen Organisationen (KMUs), die sich der Gefahren von Internet-Anwendungen und Websites bewusst sind. Das Ziel ist es, Ihnen eine Vorstellung zu geben, welche Risiken im Cyberspace existieren, und welches die besten sowie kostengünstigsten Schutz- und Vorsichtsmaßnahmen für kleine und mittelständische Unternehmen sind.

RISIKEN IM CYBERSPACE

Ist Ihnen bewusst, was geschieht, wenn Ihr Computer auf das Internet zugreift? Trotz aller erstaunlichen Dienste, Anwendungen und den Informationen, die im Internet gefunden werden können, ist es verhängnisvoll was dennoch alles passieren kann. Wenn ein Computer nicht angemessen geschützt ist, wird er kurz nachdem er eine Verbindung zum Internet aufgebaut hat von automatisierten Suchprogrammen erkannt. Dies scannen zügig alle Ports ab, die empfänglich sind für riskante Web-Anwendungen oder Malware.

Malware ist eine Computeranwendung, die absichtlich so programmiert ist, Schäden durch Datendiebstahl, Dienstverweigerung, Kontrollverlust oder Ausführung anderer Dienste anzurichten. Für Ihr Unternehmen bedeutet dies verlorene Arbeitszeit, Geld und sogar ein zerstörter guter Ruf. Die Liste dieser riskanten Web-Anwendungen beinhaltet Viren, Spyware, Botnets, Trojaner und Würmer.

Demzufolge beträgt nach Angaben des SANS Internet Storm Center (ISC) in Colorado die durchschnittliche Zeit, bis ein öffentlich zugänglicher Computer mit dem Internet verbunden wird und Ziel für einen MalwareScan wird, weniger als 20 Minuten. Bedenkt man, wie lange die meisten Menschen mit Ihrem Computer im Internet surfen oder diesen unbeaufsichtigt lassen, ist dies eine sehr kurze Zeitspanne.

Das Ponemon Institut veröffentlichte im Jahr 2010 in einer Studie, dass die durchschnittlichen Gesamtkosten eines Einbruchs in IT-Systeme im Jahr 2009 in den USA bei über \$ 6M lagen. Etwa zwei Drittel dieses Betrags kommen durch Systemstillstand bzw. aus deswegen verlorenen Geschäften zustande. Der Handel lebt heutzutage vom Internet und fast alle Unternehmen weltweit haben einen Zugang zum Internet - aber wie viele von ihnen sind vor potenziellen Bedrohungen wirklich sicher?

SICHERHEIT IM CYBERSPACE

Was können Sie also tun, um Ihr Unternehmen in einer Welt, in der sich Sicherheitsbedrohungen ständig ändern und Zeit und Ressourcen begrenzt sind, zu schützen? Die gute Nachricht ist, dass es Lösungen gibt, die die meisten Bedrohungen blockieren, noch bevor sie Ihre Systeme erreichen. Nur ausgewählte Mitarbeiter haben Zugriff auf bestimmte Websites. Ein nicht autorisierter Zugriff und Transfer von vertraulichen Unternehmensinformationen lässt sich durch den Einsatz einer defensiven Strategie mit einer starken Perimeter-Sicherheitslösung optimal eingrenzen.

DIE „IN-HOUSE“ LÖSUNG

Die verbreitete Lösung ist das „In-House-Sicherheitsmodell“, bei dem ein Unternehmen alle Geräte und Software einkauft, betreibt und verwaltet, um sich vor den Gefahren aus dem Internet zu schützen. Dieser Ansatz erfordert eine Vielzahl von Computer Hard- und Software, mit der zentral überwachte Firewalls, WebFilter, E-Mail-Filter, AntiViren- und AntiSpyware Programme regelmäßig mit diversen Updates versorgt werden. Zusätzlich überprüfen Intrusion Prevention & Detection Systeme den IP-Traffic. Diese IT-Security Systeme werden innerhalb des Unternehmens betrieben und sind mit sämtlichen Client-Geräten verbunden wie z.B. Desktop-PCs, Laptops, Tablets-PCs, Mobiltelefonen und allem, was sonst noch im Unternehmen mit dem Internet verbunden ist. Auf all diesen Endgeräten muss ein Sicherheits-Programm installiert sein. Jegliche IT-Sicherheit wird durch eine eigene IT-Service-Gruppe überwacht, betrieben und aktualisiert.

Um wirklich sicher zu sein, muss man abwägen. Es ist bestimmt attraktiv, eine Sicherheitslösung im eigenen Haus und völlig unter eigener Kontrolle zu haben - aber wie steht es um den dadurch entstehenden finanziellen Aufwand? Der offensichtliche Nachteil der Selbst-Managed-Security ist der hohe Preis. Die Inhouse-Sicherheitslösung erfordert einen physischen Schutz der Hardware. Eine Vielzahl von teuren Hardware-Geräten und Software-Paketen, die nur mit internen Experten zu installieren, zu überwachen, zu warten und zu aktualisieren sind. All diese Tätigkeiten können eine Vollzeitstelle für einen oder mehrere speziell geschulte und zertifizierte Mitarbeiter notwendig machen.

Es kann zum Problem werden, wenn man auf der einen Seite große Investitionen tätigen soll, und gleichzeitig einen Weg finden muss, um einen 24/7-Support personell und finanziell aufzubauen. Sie haben an dieser Stelle wenige Sparmöglichkeiten, weil dadurch wiederum Ihre Sicherheit leiden könnte. Wenn dies eintritt und sie eine Sicherheitslücke haben, dann kann Ihre Investition in IT-Sicherheit umsonst gewesen sein. Für die meisten KMUs machen die hohen entstehenden Investitionsausgaben mit zusätzlichen personellen Ressourcen, Rechenzentrumsstellflächen und höheren Energiekosten für ein hohes „In-House“ IT-Sicherheitsniveau unter Umständen keinen Sinn. Selbstverständlich müssen Sie mit dem Internet arbeiten können und benötigen entsprechende IT-Sicherheit – Sie müssen aber auch ein Auge auf die damit verbundenen Kosten haben. Sie sollten deswegen auch prüfen, ob es Alternativen zu einer „In-House“ Lösung gibt.

DIE „OUTSOURCING“-LÖSUNG

Ein anderer Lösungsansatz ist eine ausgelagerte IT-Sicherheitslösung (Outsourcing). Dabei wird der Internet-Verkehr von einem IT-Security-Dienstleister (Provider) mit entsprechendem Expertenwissen überwacht und mit entsprechenden Maßnahmen reagiert, wenn es erforderlich ist. Der IT-Security-Dienstleister kann die entsprechenden Geräte und Anwendungen bei Ihnen vor Ort installieren und zentral verwalten, was Ihnen Kosteneinsparungen bringt. Für noch größere Kosteneinsparungen kann Ihnen der Provider einen Internet-basierten Cloud-Dienst zur Verfügung stellen, bei dem alle IT-Sicherheits-Lösungen beim Provider virtualisiert sind und dort gehostet und verwaltet werden. „Outsourcing Security Service Provider“ kümmern sich um alle IT-Sicherheitsbelange ihrer Kunden 24/7 und an jedem Tag des Jahres. Dies beinhaltet die ständige Überwachung bzw. Monitoring, Upgrades, kontinuierliche Updates bei aktuellen Bedrohungen, Firewall-Management, E-Mail-Filterung (AntiSpam/AntiVirus), Intrusion Prevention and Detection und Web-Filtering (Proxy). Im Vergleich zur eigenen Anschaffung durch Ihr Unternehmen können diese wichtigen Tätigkeiten im Bereich IT-Sicherheit durch einen Dienstleister für einen Bruchteil der Kosten durchgeführt werden. Ihr internes IT-Personal hat wieder Zeit, sich für andere, unternehmenswichtige Aktivitäten zu kümmern, Rechenzentrumsfläche wird frei und es steht Geld für weniger ressourcenintensive Zwecke zur Verfügung.

DIE INDEVIS-LÖSUNG: EIN CLOUD FIREWALL SERVICE

Die ausgelagerte IT-Security-Lösung von indevis – ein Cloud Firewall Service (CFS) – bietet umfassenden Schutz für Ihr Unternehmen, ohne großen Investitionsaufwand und einem ganzen Stab von Internet-Security-Experten. Ein CFS bietet einen zentralen, redundanten Firewall-Knoten, der Ihr Unternehmen vor Schäden und gefährlichen Internet-Schädlingen überwacht und schützt.

Der Dienst ist in verschiedenen Ausführungen erhältlich, der genau Ihren Bedürfnissen angepasst werden kann, er kann folgendes enthalten*:

1. Eine Firewall die Applikationen erkennen und filtern kann
2. Website/URL-Filtering
3. Anti-Virus und Anti-Spyware
4. Intrusion Detection and Prevention (IPS)
5. File Filtering / Data Loss Prevention (DLP)
6. Benutzerdefinierte Berichte und Dokumentation
7. VPN-Client für Remote-Benutzer
8. Zero-Day Attack Protection

*Diese Funktionen werden im Folgenden ausführlich beschrieben.

1. EINE FIREWALL DIE APPLIKATIONEN ERKENNEN UND FILTERN KANN

Eine Firewall die Applikationen erkennen kann – also eine Firewall der nächsten Generation – ist wesentlich besser als eine herkömmliche Firewall, wie sie in vielen In-House Installationen im Einsatz ist. Unser Cloud Firewall Service bietet beides: Sichtbarkeit jeder Anwendung und Kontrolle jeder Anwendung. Durch die Anwendungstransparenz haben Sie die Möglichkeit Anwendungen zu identifizieren, und zu sehen, welcher Mitarbeiter welche Internetanwendung verwendet. Sie können dann festlegen, ob Sie die Nutzung bestimmter Anwendungen zum Schutz Ihres Netzwerks und zur Produktivitätssteigerung Ihrer Mitarbeiter einschränken möchten. Die Applikationskontrolle ermöglicht es Ihnen, Web-Anwendungen mit hohem Risiko sowie riskantem Verhalten zu blockieren. Das Ergebnis ist ein deutlich sichereres Unternehmensnetzwerk und optimierte Bandbreite für geschäftskritische Aktivitäten.

Werfen Sie einen Blick auf die Risiken, die von Peer-to-Peer File-Sharing Websites und Plattformen ausgehen. Sie riskieren die Verletzung von Urheberrechtsgesetzen und bieten evtl. Spyware oder Viren ein Einfallstor in Ihr Netzwerk. Diese Seiten haben sowohl das Potenzial Malware in Ihr Netzwerk zu transferieren, als auch die Möglichkeit vertrauliche Daten aus Ihrem Netz zu schleusen, von denen Sie sicherlich nicht möchten, dass sie Ihr Netz verlassen. Mit einer Firewall, die Applikationen erkennen und kontrollieren kann, können Sie alle Arten von hoch riskanten web-basierten Anwendungen verhindern, die möglicherweise zusätzlich die Effizienz Ihres Unternehmens untergraben.

2. WEBSITE/URL-FILTERING

Der CFS-Website-Filter blockiert den Zugriff oder warnt den Anwender vor dem Zugriff auf ungeeignete Websites. Diese Komponente schützt Ihr Unternehmen vor diversen rechtlichen, regulatorischen und produktiven Risiken. Dieser URL-Filter wird ständig durch indevis aktualisiert und gepflegt.

Damit lassen sich z.B. Multi-Player-Spiele-Websites (z.B. World Of Warcraft) blockieren, die in der Regel in einem Unternehmensnetzwerk nichts verloren haben. Statt während der Arbeitszeit zu spielen, blockiert der CFS den Zugang. In Verbindung mit der Applikationskontrolle und andere Komponenten, wie z.B. einer schwarzen Liste von Web-Adressen und einer Filterung-Datenbank, verhindert der CFS-Website-Filter den Besuch von Websites, welche die Firmensicherheit untergraben und den Arbeitsplatz eines Kollegen gefährden können.



3. ANTI-VIRUS UND ANTI-SPYWARE

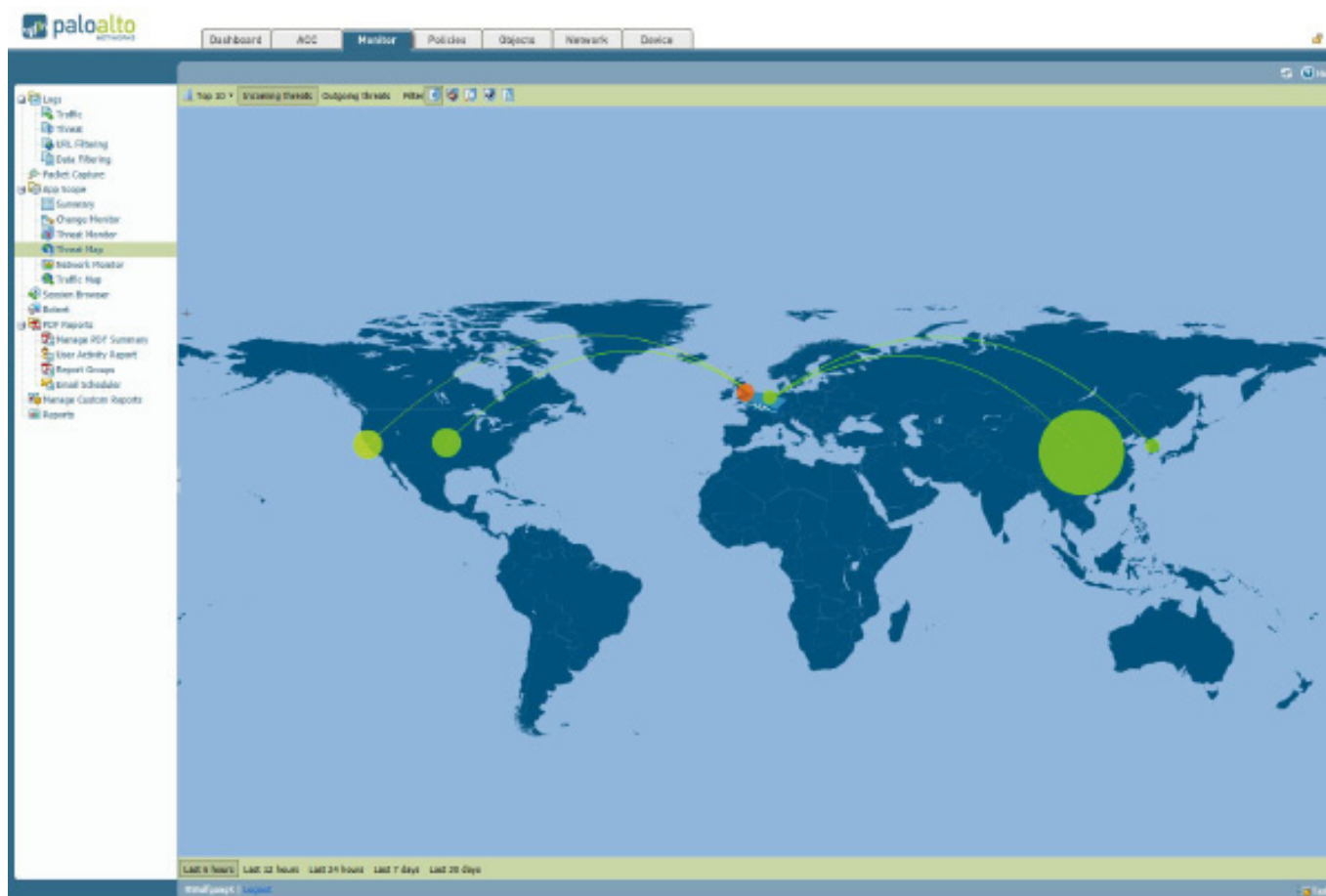
Diese Funktion verhindert, dass Millionen von Malware-Varianten in Ihr Netzwerk eindringen können. Dazu gehört auch ein Dienst, der versteckte Viren und schadhafte Codes im Web-Datenverkehr stoppt. Anti-Virus und Anti-Spyware schützt Ihr Netzwerk vor unbefugtem und bösartigem Zugriff, der zu verlorener Zeit und Geld - und sogar dem Verlust von Daten führen kann.

Befindet sich zum Beispiel ein Virus in einer HTML-Grafik einer scheinbar sicheren Website, verbreitet sich der Virus auf jeden Computer, der die Website besucht. Wenn allerdings ein CFS im Einsatz ist, wird die Malware am Gateway erkannt und blockiert.

4. INTRUSION DETECTION UND PREVENTION (IPS)

Die CFS Intrusion Detection und Prevention identifiziert und blockiert Angriffe auf Netzwerk- und Applikationsebene, die folgende Schwachstellen ausnutzen: Puffer Overflows, Denial-of-Service-Angriffe und Port-Scans. Ähnlich wie die Anti-Viren- und Anti-Spyware-Funktion beschützt die Intrusion Detection und Prevention Funktion Ihr System vor gefährlichen, unbefugten Zugriffen. Dadurch spart sich Ihr Unternehmen teure Netzwerk-Unterbrechungen oder -Ausfälle und verlorene Daten.

Denken Sie beispielsweise an ein Unternehmen, das an einem bestimmten Tag ein neues Produkt launchen möchte, dessen Website aber von einer Denial-of-Service-Angriff angegriffen wird und deswegen nicht mehr verfügbar ist. Die IPS-Funktion der Firewall erkennt und blockiert die DoS-Angriffe und hält sie von dem Firmen-Netzwerk und der Website fern – alles arbeitet normal weiter.



5. FILE FILTERING / DATA LOSS PREVENTION (DLP)

Der CFS „Daten-Filterung/DLP“ überwacht die datei-übertragenden Funktionen der einzelnen Anwendungen. Er erlaubt einem Programm das Ausführen seiner Aufgaben, sorgt aber dafür, dass keine gefährlichen Dateien übertragen werden. E-Mail-Anhänge, Downloads und Uploads über Webportale werden registriert und evtl. verweigert.

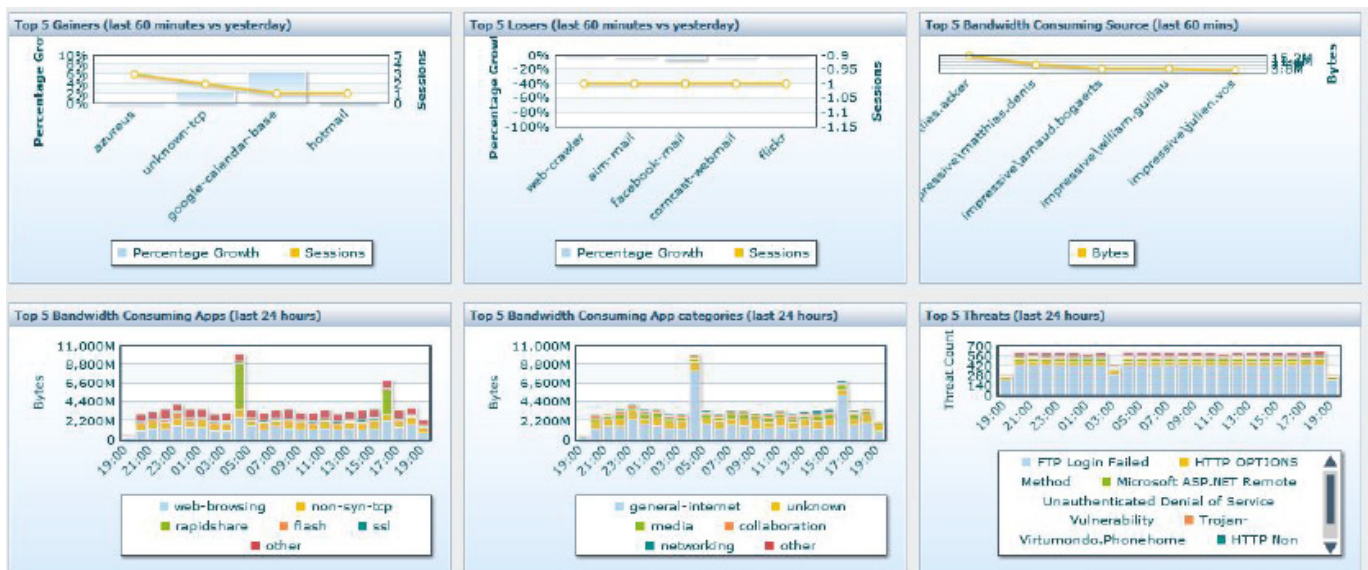
Betrachten Sie zum Beispiel einen Mitarbeiter, der versuchen könnte über sein persönliches Hotmail E-Mail-Konto Dateien (z.B. Tabellenkalkulationen, Kundendaten, etc.) aus Ihrem Netzwerk zu versenden. Unsere Firewall kann beispielsweise die Verwendung von Hotmail erlauben, aber sie kann verhindern, dass XLS-Dateien mit möglicherweise proprietären Unternehmensinformationen das Unternehmensnetz auf diesem Weg verlassen.

6. BENUTZERDEFINIESTE BERICHTE UND DOKUMENTATION

Der CFS liefert detailliert zusammenfassende Berichte über Aktivitäten und Bedrohungen. Diese Berichte beinhalten „Change Reports“, Bedrohungs-Monitor, Netzwerk-Monitor, Top-Applikationen und Top-High-Risk-Anwendungen. Die Informationen sind leicht verständlich und liefern wichtige Informationen zu den Verursachern möglicher Bedrohungen und Angriffe. Somit ist eine schnell Zustandsbewertung der Netzwerksicherheit möglich.

Benutzerdefinierte Berichte und Dashboards lassen sich ebenfalls erstellen. Unser Cloud Firewall Service ermöglicht es Kunden selbst Policies hinzuzufügen, zu ändern oder zu löschen. Ihre IT-Sicherheits-Richtlinien können Sie selbst am Perimeter festlegen – ganz nach Ihrem Anforderungsprofil.

Zum Beispiel erhalten Sie eine knappe graphische Zusammenfassung für Ihren IT-Leiter oder für die Geschäftsleitung, um sich schnell einen Überblick über das Netzwerk zu verschaffen. Unsere Firewall liefert Ihnen Berichte in beliebiger Detailtiefe – je nachdem wen Sie damit adressieren möchten.



7. VPN-CLIENT FÜR REMOTE-BENUTZER

Die meisten Unternehmen zwingen Ihre Remote-Benutzer auf deren Laptops einen VPN-Client zu verwenden, um ihr Firmennetz vor Malware zu schützen. Unser CFS bietet einen sicheren Remote-VPN-Client für mobile Benutzer und ermöglicht somit einen sicheren Zugang auf Ihre Netzwerk-Ressourcen.

Beispielsweise nutzt ein Mitarbeiter einen VPN-Client, um von Zuhause aus zu arbeiten und auf das Firmennetz zuzugreifen. Wenn er eine riskante Anwendung aufruft, die möglicherweise durch Unternehmensrichtlinien nicht erlaubt ist, oder als „infiziert“ erkannt wird, wird diese Aktion blockiert. Hätte er nicht den VPN-Client verwendet, wäre der Zugriff auf die infizierte Anwendung nicht gesperrt worden, und der schadhafte Code hätte sich im Netzwerk unkontrolliert verbreiten können.

8. ZERO-DAY ATTACK PROTECTION

Zero-Day Attacken und Angriffe mit Malware werden zunehmend zum Problem für Unternehmen. Malware wird durch unachtsames öffnen von infizierten E-Mails oder dem Surfen im Web auf infizierten Webseiten in Unternehmensnetzwerke eingeschleppt – eine „Botnetz-Infektion“ ist schnell passiert. Mit unserer Technologie überprüfen wir jegliche Art von IP-Traffic der Ihr Netz verlässt und spüren somit unerwünschte Verbindungen auf und blocken diese sog. „Callbacks“.

FAZIT

Der indevis Cloud Firewall Service liefert Ihnen ein hochsicheres Umfeld für Ihren Unternehmens-Internet-Zugang. Das System ist speziell entwickelt und designed worden, um Ihr Unternehmen deutlich sicherer zu machen und um es vor den zunehmenden Internet-Bedrohungen zu schützen. Da Malware-Angriffe immer komplexer werden und sich ständig verändern, brauchen Unternehmen unbedingt eine sichere Lösung, die robust genug ist und bleibt, und die den permanenten, bösartigen Angriffen gewachsen ist. Unser Cloud-Firewall-Dienst ist ein umfassender outgesourcter Internet-Security-Service, der für einen Bruchteil der Kosten im Vergleich zu einer Inhouse-Security-Lösung bereitgestellt werden kann. Sie können sich auf indevis verlassen. Wir überwachen Ihr Netzwerk und aktualisieren unsere Dienste um Ihr Netzwerk nachhaltig vor Bedrohungen aus dem Internet zu verteidigen.

ÜBER INDEVIS

Die indevis GmbH ist ein international, national und regional tätiges Unternehmen auf dem Feld der Informationstechnologie und Netzwerkkommunikation, das Lösungen und Dienste für sichere Datennetze anbietet, welche alle Anforderungen sowohl der Wirtschaft als auch von öffentlichen Behörden und Hochschulen erfüllen.

Unsere Kunden unterstützen wir in der Analyse, Konzeptionierung, Realisierung, Betrieb und Betriebsunterstützung von IT-Sicherheits- und -Netzwerkinfrastruktur und Informationssicherheit.

Seit 1999 versteht sich die indevis GmbH als Lösungsanbieter für komplexe IT-Sicherheits- und Netzwerk-Infrastrukturen und steigert die Effizienz von Organisationen in den verschiedensten Branchen.

Zu unseren zufriedenen Kunden zählen namhafte Unternehmen in den Bereichen:

- Automobil- und Zulieferindustrie
- Beratungsunternehmen (RAe, WP, StB, UB, PAe)
- Dienstleistungsunternehmen
- Fertigungsindustrie
- Finanzdienstleister
- Gesundheitswesen
- Lebensmittelindustrie
- Maschinenbau
- Medizintechnik
- Öffentliche Hand/Verwaltung/Behörden
- Universitäten, Hochschulen und Wissenschaft

indevis versteht sich als Partner dieser Organisationen, der seinen Kunden Lösungen für sichere Netzwerke bietet oder ihm komplexe Netzwerkaufgaben abnehmen kann. Dies wird durch professionelle Management- und Supportdienste abgesichert. Ziel von indevis ist es Ihnen eine perfekte Beratung zu unseren sehr guten Produkten, Dienstleistungen und neuester Technologie zu liefern – zu wettbewerbsfähigen, fairen Preisen! Seit 1999 machen und verstehen wir dieses Geschäft.

Weitere Informationen zu unseren Produkten und Dienstleistungen finden Sie im Internet unter:

www.indevis.de

Kontaktperson: Herr Andreas Mayer

Telefon: +49 (89) 45 24 24-100

E-Mail: sales@indevis.de