
CYBER
SECURITY
DER NÄCHSTEN GENERATION.
BEI iT-CUBE.
SCHUTZ FÜR DAS MODERNE
UNTERNEHMEN UND SEINE MITARBEITER.
Teilnehmer der
Allianz für
Cyber-Sicherheit
proofpoint.
iT-CUBE
SYSTEMS
Member of SecureLink

HEUTIGE BEDROHUNGEN FÜR ORGANISATIONEN.

Der Mensch ist das schwächste Glied in der Sicherheitskette. Angriffe zielen verstärkt über verschiedene Vektoren auf menschliche statt auf systemtechnische Schwächen. Diese Attacken können nur mit Lösungen abgewehrt werden, die umfassenden **SCHUTZ AUCH VOR ADVANCED THREATS** bieten.

DIE LÖSUNG.

PROOFPOINT schützt Unternehmen und Mitarbeiter vor hochentwickelten und gezielten Angriffen über verschiedene Kommunikationskanäle, wie E-Mail, Mobile Apps oder Social Media und unterstützt, Compliance-Richtlinien einzuhalten.

Sollte ein Angriff erfolgreich sein, können Bedrohungen schnell und zuverlässig eingedämmt werden.

DAS DREISTUFIGE PROOFPOINT SICHERHEITS KONZEPT

IN EINER ZENTRALEN PLATTFORM.

1 PROOFPOINT ENTERPRISE PROTECTION

Blockiert bekannte Bedrohungen und ungewollte E-Mails (Anti Spam, Anti Virus, bekannter Phish, etc.)

2 PROOFPOINT TARGETED ATTACK PROTECTION

Blockiert unbekannte Bedrohungen und APTs durch zielgerichtete Attacken via Phish.

3 PROOFPOINT THREAT RESPONSE

Incident Response Management zur effizienten Reaktion auf Sicherheitsvorfälle und Infizierungen.

PROOFPOINT ENTERPRISE PROTECTION

RUNDUMSCHUTZ

VOR E-MAIL BASIERTEN BEDROHUNGEN.

Proofpoint Enterprise Protection liefert effektiven **SCHUTZ VOR E-MAIL-BEDROHUNGEN**, einschließlich Phishing, Malware, Spam und anderen Formen von inakzeptablen oder gefährlichen Inhalten. Die Proofpoint Enterprise Protection™-Suite bietet für eingehende und ausgehende E-Mails branchenführende Sicherheits- und Verwaltungsfunktionen in einer einzigen kostengünstigen, benutzerfreundlichen Lösung.

- **HÖCHSTE E-MAIL-SICHERHEIT:**
  Phishing-Schutz, Anti Spam, Anti Virus, Durchsetzung von E-Mail-Richtlinien
- **TIEFE INHALTSANALYSE:**
  Akkurate Bedrohungs-Klassifizierung durch Proofpoint MLX™* für Phishing, Spam oder Malware
- **MEHRSTUFIGER VIRENSCHUTZ**
  durch signaturbasiertes Anti Virus und verhaltensbasierten Zero Hour-Schutz
- **DYNAMIC-REPUTATION-SERVICE**
  für Global IP- und URL-Reputation
- **INDIVIDUELLES RICHTLINIEN-MANAGEMENT**

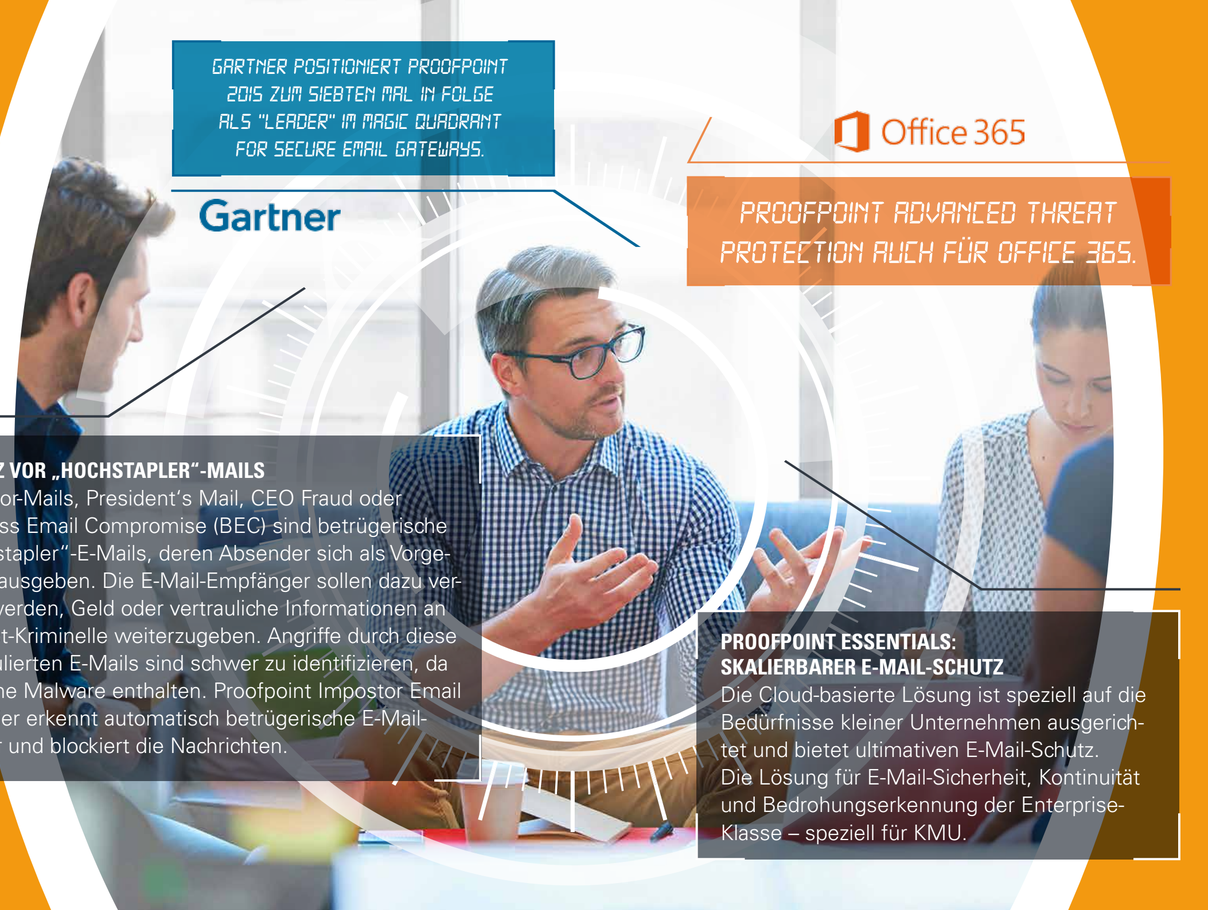
*Patentierte Proofpoint Technologie für maschinelles Lernen

GARTNER POSITIONIERT PROOFPOINT 2015 ZUM SIEBTEN MAL IN FOLGE ALS "LEADER" IM MAGIC QUADRANT FOR SECURE EMAIL GATEWAYS.

Gartner

Office 365

PROOFPOINT ADVANCED THREAT PROTECTION AUCH FÜR OFFICE 365.



SCHUTZ VOR „HOCHSTAPLER"-MAILS
Impostor-Mails, President's Mail, CEO Fraud oder Business Email Compromise (BEC) sind betrügerische „Hochstapler"-E-Mails, deren Absender sich als Vorgesetzte ausgeben. Die E-Mail-Empfänger sollen dazu verleitet werden, Geld oder vertrauliche Informationen an Internet-Kriminelle weiterzugeben. Angriffe durch diese manipulierten E-Mails sind schwer zu identifizieren, da sie keine Malware enthalten. Proofpoint Impostor Email Classifier erkennt automatisch betrügerische E-Mail-Muster und blockiert die Nachrichten.

PROOFPOINT ESSENTIALS: SKALIERBARER E-MAIL-SCHUTZ
Die Cloud-basierte Lösung ist speziell auf die Bedürfnisse kleiner Unternehmen ausgerichtet und bietet ultimativen E-Mail-Schutz. Die Lösung für E-Mail-Sicherheit, Kontinuität und Bedrohungserkennung der Enterprise-Klasse – speziell für KMU.

PROOFPOINT TARGETED ATTACK PROTECTION

EFFEKTIVE VERTEIDIGUNG

GEGEN GEZIELTE ANGRIFFE.

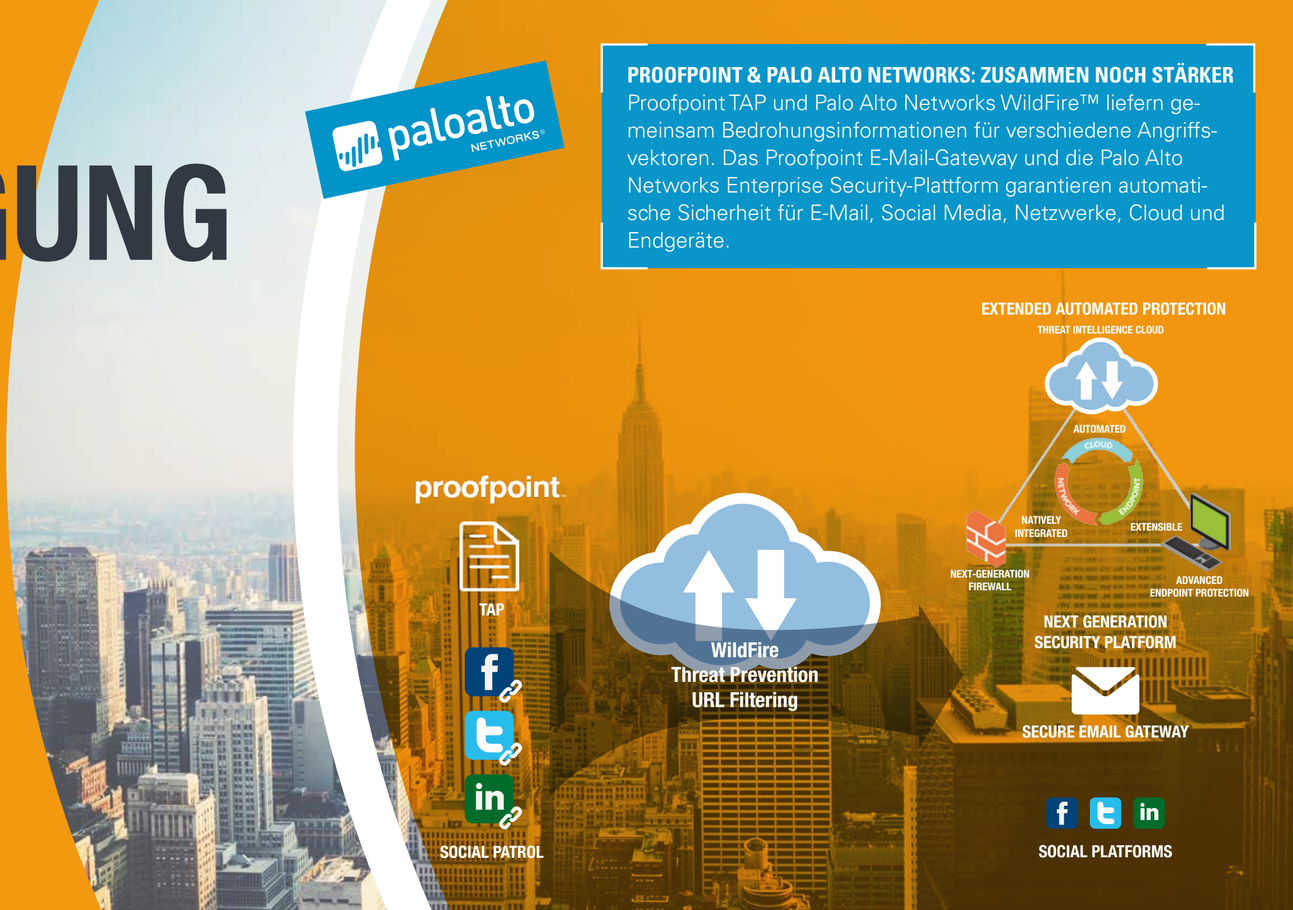
Gezielte Spear-Phishing-Kampagnen sind eines der Hauptprobleme von Sicherheitsbeauftragten. Proofpoint Targeted Attack Protection (TAP) bildet normales E-Mail-Verhalten in seiner Sandbox-Umgebung ab, um Anomalien zu erkennen.

So werden auch einzelne Mails, die zu einer gezielten Attacke führen können, aus dem kompletten Mail-Aufkommen eines Unternehmens herausgefiltert.

- **DYNAMISCHE ECHTZEIT-ANALYSE UND -BLOCKIERUNG**
  von schadhaften URLs und Anhängen, die Anti Viren- und Reputationsfilter umgehen
- **VORAUSSCHAUENDER SCHUTZ:**
  Erkennung gefährlicher URLs in unerwünschten E-Mails und Blockierung von Benutzerklicks
- **UMFASSENDE SICHERHEIT**
  inner- und außerhalb des Netzwerkes: Follow Me-Schutz verfolgt Mails und prüft die Sicherheit von URL-Zielen in Echtzeit
- **END-TO-END-EINBLICK:**
  Erkennt Gefährdungen und beschleunigt die Reaktionszeit bei Phishing- und Webmanipulationsangriffen, durch die schnelle Identifizierung von Kampagnen, anvisierten Benutzern und potenziell infizierten Systemen

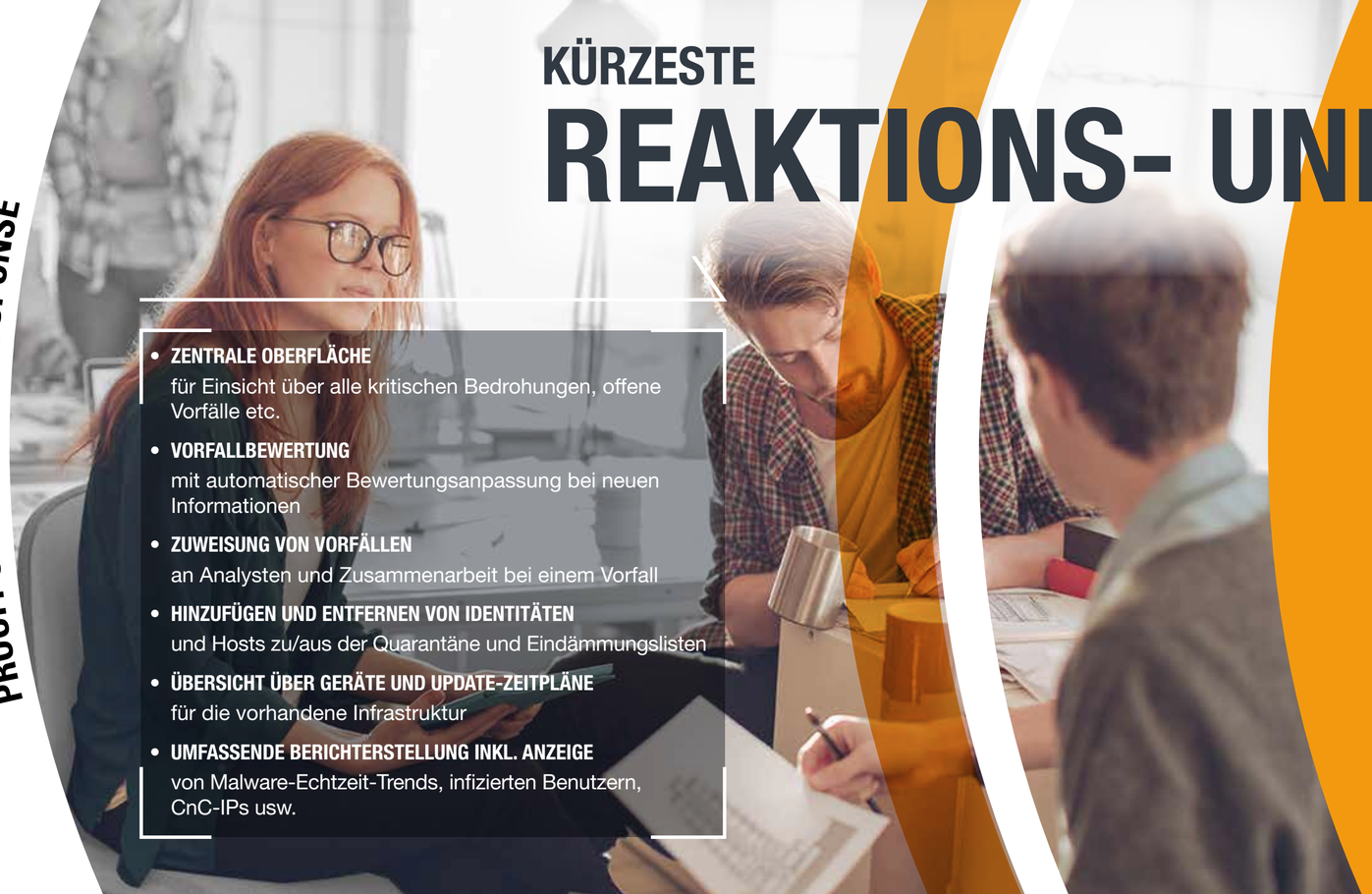
paloalto NETWORKS

PROOFPOINT & PALO ALTO NETWORKS: ZUSAMMEN NOCH STÄRKER
Proofpoint TAP und Palo Alto Networks WildFire™ liefern gemeinsam Bedrohungsinformationen für verschiedene Angriffsvektoren. Das Proofpoint E-Mail-Gateway und die Palo Alto Networks Enterprise Security-Plattform garantieren automatische Sicherheit für E-Mail, Social Media, Netzwerke, Cloud und Endgeräte.



PROOFPOINT THREAT RESPONSE

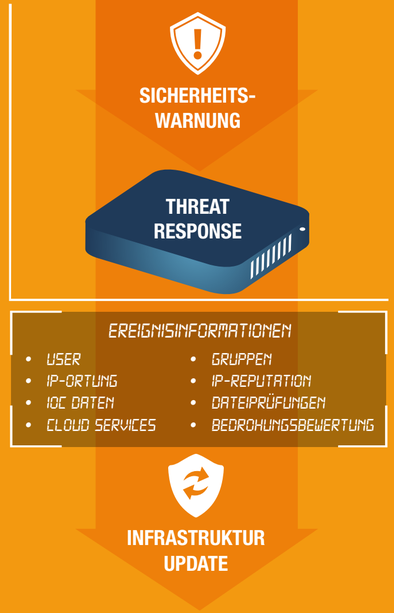
KÜRZESTE REAKTIONS- UND ABWEHRZEITEN BEI BEDROHUNGEN.



- **ZENTRALE OBERFLÄCHE**
  für Einsicht über alle kritischen Bedrohungen, offene Vorfälle etc.
- **VORFALLBEWERTUNG**
  mit automatischer Bewertungsanpassung bei neuen Informationen
- **ZUWEISUNG VON VORFÄLLEN**
  an Analysten und Zusammenarbeit bei einem Vorfall
- **HINZUFÜGEN UND ENTFERNEN VON IDENTITÄTEN**
  und Hosts zu/aus der Quarantäne und Eindämmungslisten
- **ÜBERSICHT ÜBER GERÄTE UND UPDATE-ZEITPLÄNE**
  für die vorhandene Infrastruktur
- **UMFASSENDE BERICHTERSTELLUNG INKL. ANZEIGE**
  von Malware-Echtzeit-Trends, infizierten Benutzern, CnC-IPs usw.

PROOFPOINT THREAT RESPONSE ermöglicht die schnelle Identifikation, Blockade und Deaktivierung von Angriffen und zuvor unerkannter Malware, die sich bereits eingenistet hat.

Die Lösung ist die zentrale Threat Management-Plattform zum automatisierten Incident Management bei Sicherheitsvorfällen. Threat Response reichert Sicherheitswarnungen verschiedener Systeme mit Hintergrundinformationen an, um verwertbare Daten zu generieren, prüft die Infektion von Systemen (IOC) und vergleicht sie automatisch mit den forensischen Informationen der eingesetzten Sandbox-Lösung. Auf Knopfdruck oder automatisiert können daraufhin Aktivitäten zur Abwehr von Bedrohungen ausgelöst werden.



COMPLIANCE MIT PROOFPOINT

LÖSUNGEN FÜR VIER WESENTLICHE HERAUSFORDERUNGEN VON ORGANISATIONEN.

DATENVERLUST VERHINDERN

Der Verbleib sensibler Informationen muss transparent sein. Diese Daten dürfen Unternehmen nicht ungewollt verlassen! **Proofpoint Data Loss Prevention (DLP)** vereinfacht die Suche und Bewertung von Daten, setzt Richtlinien zentral und konsequent durch und leitet regelwidrige Daten automatisch um.

SICHERE KOMMUNIKATION

Proofpoint Encryption ermöglicht den automatischen, verschlüsselten Versand sowohl richtlinienkonformer E-Mails als auch solcher, die im Falle eines Fehlers oder einer Datensicherheitsverletzung auf Empfängerseite, widerrufen werden müssen. Mit Proofpoint können Unternehmen ihre Informationen auch außerhalb der Unternehmensgrenzen kontrollieren.

KONTROLLE DER DATENVERTEILUNG

Proofpoint Enterprise Content Control erkennt und verfolgt mit performanten Richtlinienkontrollen die Bewegung sensibler Daten, bevor ein möglicher Datenverlust eintritt. Das Risiko von Datenverlusten wird minimiert und das Nutzerverhalten nachvollziehbar.

EINHALTUNG GESETZLICHER RICHTLINIEN

Mit **Proofpoint Enterprise Archive** können Anwender Mails, Dateien, Chats, Social-Media-Kommunikation und mehr archivieren und binnen 20 Sekunden durchsuchen. Proofpoint verfolgt auch Dateien nach, die z.B. zwischen Mail-Postfächern und Desktops oder SharePoint bewegt werden. Nachweise für den Compliance-Beauftragten sind jederzeit verfügbar.

ERWEITERTER SCHUTZ

SCHUTZ VOR ANGRIFFEN ÜBER MOBILE APPS

Proofpoint Targeted Attack Protection (TAP) Mobile Defense blockiert schädliche Apps für Android™ und iOS®. Durch die enge Einbindung in führende Enterprise Mobility Management-Plattformen wie MobileIron® und VMware AirWatch® entfernt TAP Mobile Defense schädliche Apps auch vorbeugend. TAP Mobile Defense nutzt die fortschrittliche Sandbox-Funktion von Proofpoint TAP zur Anomalie-Erkennung und schützt auch vor ausgeklügelten, zielgerichteten Angriffen.

ÜBERWACHUNG UND SCHUTZ FÜR SOCIAL MEDIA-KONTEN

Proofpoint Nexgate überwacht Social Media-Konten von Unternehmen. Twitter, Facebook, LinkedIn und andere Konten werden gescannt, mit der eigenen Marke verbundene Konten gefunden und überprüft. Die Lösung verwaltet Zugänge und verbundene Anwendungen, filtert beleidigende oder anstößige Inhalte, archiviert Kommunikationen und verhindert Betrug oder Account-Hacking.

THREAT INTELLIGENCE FÜR PROAKTIVE ABWEHR

Proofpoint ET Intelligence™ führt minutengenaue IP- und Domain-Reputationsinformationen in einer Datenbank von weltweit beobachteten Bedrohungen und Malware-Analysen zusammen. Die branchenweit aktuellste und genaueste Quelle für Bedrohungsinformationen unterstützt IT-Sicherheitsverantwortliche, schädliche Angriffe proaktiv abzuwehren und liefert Kontext-Informationen zur Analyse.

Proofpoint bei iT-CUBE.

HABEN SIE DIE KONTROLLE ÜBER IHREN E-MAIL-VERKEHR?

TESTEN SIE IHRE TAKTIK!

4-wöchiger Double Check Service für Ihre E-Mails:

- Prüfung Ihres E-Mail-Verkehrs parallel zu Ihrer vorhandenen Sicherheitslösung mit Proofpoint.
- Integration in Ihre bestehende Sicherheitslösung*
- kontinuierliche Analyse & Auswertung der Incidents
- Abschlussreport mit allen Analysen samt Bewertung
- Beratung & Unterstützung bei Ihrer Security-Strategie

*Splunk / Palo Alto Networks / Imperva / CyberArk

+49 (0)89 2000 148 00

INFO@IT-CUBE.NET

WWW.IT-CUBE.NET/PROOFPOINT

SCHLECHTE KARTEN ...FÜR FALSCHSPIELER.

iT-CUBE SYSTEMS AG
Paul-Gerhardt-Allee 24
81245 Munich, GERMANY
Phone: +49 (0)89 2000 148 00
Mail: info@it-cube.net
Web: www.it-cube.net