Wir ERSPAREN Ihnen SPAM und ENTFERNEN VIREN -

BEVOR Emails Ihr Netzwerk erreichen!

Damit Sie sich nicht mehr vor den Gefahren des Internets verteidigen müssen, machen wir das ab sofort für Sie.

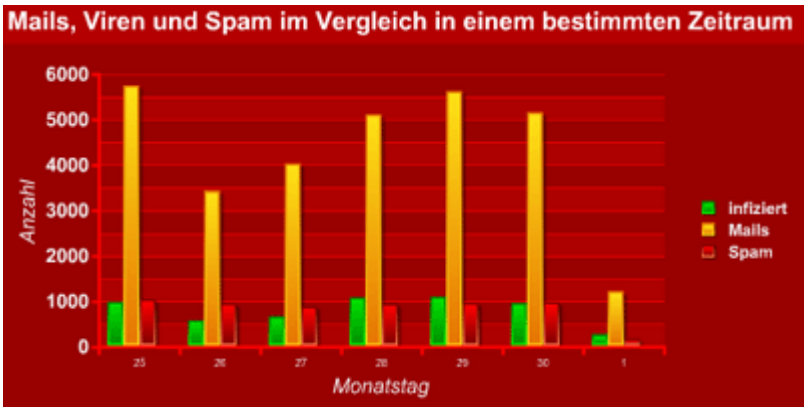
Die **IKARUS Managed Security Services** filtern sämtliche Computerviren, Spammails, etc. aus Ihrem Mailverkehr, bevor diese Ihr Unternehmen erreichen. Parallel dazu wird dieses System rund um die Uhr von Experten überwacht, die gleichzeitig weltweit nach neuen digitalen Gefahren Ausschau halten, und Sie im Falle des Falles davor bewahren.

Wir ENTFERNEN VIREN und ERSPAREN Ihnen SPAM,
BEVOR Emails Ihr Netzwerk erreichen!

IKARUS Managed Security Services (MSS) bieten Ihnen die Möglichkeit, Ihre Emails auf Computerviren und Spam zu überprüfen, bevor diese Ihr Netzwerk erreichen.

Ihre Vorteile:

- Keine Softwareinstallation
- Individuelle Konfiguration
- Höchste Ausfallsicherheit
- Keine Hardwareanschaffungen
- Keine Wartung



- IKARUS Software übernimmt dies alles für Sie!

Mittlerweile vertrauen 1000de Unternehmen auf die Leistung der IKARUS Managed Security Services. Sogar Internetprovider, Banken und Versicherungen schicken mittlerweile den gesamten Emailtraffic in unser IKARUS Scan Center um eine verlässliche Prüfung auf Viren und Spams zu gewährleisten.

Was sind Managed Security Services?

Infolge der größen Zunahme von Gefahren aus dem Internet, sehen sich Unternehmen nicht mehr in der Lage, ihre Systeme ausreichend zu schützen. Deshalb lagern sie immer öfter diese Aufgaben an externe Spezialisten aus, die kostengünstiger und effektiver diese Aufgabe übernehmen können. Bei IKARUS Managed Security Services übernehmen Experten diese Aufgaben, um Sie vor Computerviren und Spam zu schützen.

FUNKTIONEN die jedem Kunden über ein persönliches Webinterface zur Verfügung stehen:

- **Antivirus Funktionen** (entfernen, löschen, Warnungen, etc.)
- **Antivirus Statistiken** (flashanimiert)
- **Free Removertools** (Falls Sie auf anderem Weg einen Virus erhalten haben)
- **Blacklist- und Whitelist** (Filterlisten für Dateiextensions, etc.)
- **Antispamfunktionen** (Intensität, selbst definierbare Spamregeln, etc.)
- **Antispamstatistiken** (flashanimiert)
- **Logeinträge** (Größe, Anzahl der Emails, etc.)

- **Alerting** (Wer soll Wann Wie alarmiert werden)

Funktionsweise:

Ihre eingehenden Emails werden vom IKARUS Scan Center entgegengenommen, und auf Computerviren und/oder Spam überprüft. Anschließend werden Ihnen die gereinigten Emails zugestellt. Sie selbst können die Konfiguration über ein Webinterface ändern, sowie die entsprechenden Statistiken zur Überprüfung der Effektivität abrufen.

Beschreibung IKARUS Scan Center:

Das IKARUS ScanCenter wird am VIX-2 in Wien gehostet, und von IKARUS Mitarbeitern upgedatet, gewartet und überwacht. Die Sicherheit wird durch geclusterte Firewalls gewährleistet. Technologien wie gehärtete Betriebsysteme, physikalisch getrennte VLANs, High Availability mit Hilfe von hot standby failovers, Heartbeat Monitoring etc. sind Fakten die nicht nur KMUs überzeugen sondern auch große Unternehmen wie Banken und Versicherungen. Mittlerweile schicken bereits einzelne ISPs ihren kompletten Emailtraffic über das IKARUS Scan Center um vor Computerviren und Spam sicher zu sein.

ANTIVIRUS - FILTERING:

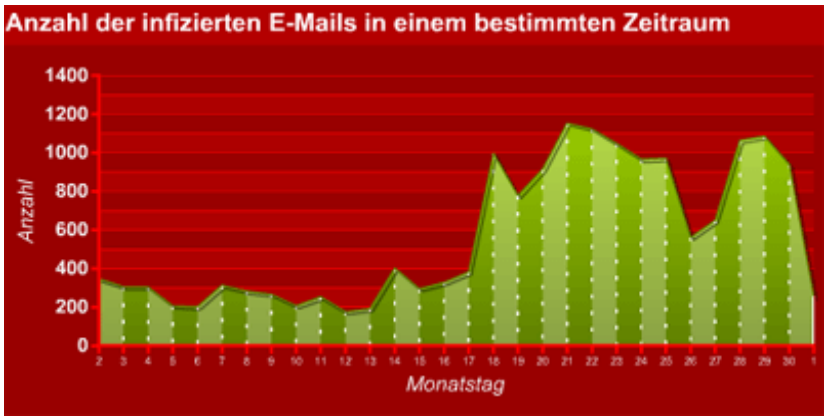
Effektive Scantechnologie:
Die IKARUS Managed Security Services verwenden den IKARUS T3 Scanner, der eine fast 100%ige Erkennungsrate erreicht. Gescannt wird nach Computerviren, Trojanern, Würmern, Active-x, Scripts, malicious Code, Java Applets, etc.

Second Level Scanner:
Wird bereits ein Virenscanner im Unternehmen eingesetzt, ist die IKARUS Managed Security Services die ideale Lösung als Second Level Scanner - denn 4 Augen sehen mehr als 2!

Virensupport und Konfigurationssupport:
IKARUS Kunden steht Support bei der Konfiguration der IKARUS Managed Security Services, sowie Support bei Problemen mit Computerviren zur Verfügung. Supportzeiten: Montag-Freitag von 08:00 - 18:00.

SPAM - FILTERING:

Schonung der Bandbreite und keine Verschwendung von Arbeitszeit:
Mittlerweile übersteigt der Anteil der Spams am gesamten Emailtraffic bereits über 50%. Dieser Prozentsatz wird in den kommenden Jahren noch weiter steigen. Mit IKARUS Managed Security Services werden bis zu 98% aller Spams gefiltert. D.h. das bringt einerseits eine spürbare Entlastung Ihrer Internetanbindung, andererseits verschwenden Ihre Mitarbeiter keine Zeit mehr für das Überprüfen von Emails. Was dies genau an



Ersparnis im Bereich der Arbeitszeit bringt, können Sie auf unserer Homepage mit dem **Spam - Calculator** einfach ausrechnen.

Spamfiltering- TECHNOLOGIEN:

Mittels verschiedenster Methoden und selbstlernender Algorithmen werden Emails nach vielen Regeln bewertet und je nach Ihrer Konfiguration weiterverarbeitet (löschen, markieren oder redirekten). Die Sensibilität des Spamfilters kann von low bis high in 9 Unterstufen von Ihnen eingestellt werden. Zusätzlich können Sie selbst Regeln und deren Sensibilität definieren, mit der Sie die Suche nach Spam verfeinern können.

Pro

ANTIVIRUS - FILTERING:

Effektive Scantechnologie:
Die IKARUS Managed Security Services verwenden den IKARUS T3 Scanner, der eine fast 100%ige Erkennungsrate erreicht. Gescannt wird nach Computerviren, Trojaner, Würmer, Active-x, Scripts, malicious Javaspplets, etc...

Second Level Scanner:
Wird bereits ein Virenscanner im Unternehmen eingesetzt, ist IKARUS Managed Security Services die ideale Lösung als Second Level Scanner - denn 4 Augen sehen mehr als 2!

Virensupport und Konfigurationssupport:
IKARUS Kunden haben natürlich Support bei der Konfiguration der IKARUS Managed Security Services , sowie Support bei Problemen mit Computerviren. Supportzeiten: Montag - Fritag von 08:00 - 18:00.

SPAM - FILTERING:

Schonung der Bandbreite und keine Verschwendung von Arbeitszeit:
Mittlerweile übersteigt der Anteil der Spams am gesamten Emailtraffic durchschnittlich bereits über 50%. Dieser Prozentsatz wird in den kommenden Jahren noch gewaltig steigen. Mit IKARUS Managed Security Services können bis zu 98% aller Spams erkannt und gelöscht werden. D.h. lästige Spams werden ausgefiltert, bevor sie Ihr Gateway erreichen. Dies bringt einerseits eine spürbare Entlastung Ihrer Internetanbindung, andererseits verschwenden Ihre Mitarbeiter keine Zeit mehr für das Überprüfen von Emails. Was dies genau an Ersparnis im Bereich der Arbeitszeit bringt, können Sie auf unserer Homepage mit dem **SPAM - CALCULATOR** einfach erheben.

Spamfiltering- TECHNOLOGIEN:

Mittels verschiedenster Methoden und selbstlernenden Algorithmen werden Emails nach vielen Regeln bewertet und je nach Ihrer Konfiguration weiterverarbeitet (löschen, markieren oder redirekten). Die Sensibilität des Spamfilters kann von low bis high in 9 Unterstufen von Ihnen eingestellt werden. Zusätzlich können Sie selbst Regeln und deren Sensibilität definieren, mit der Sie die Suche nach Spam verfeinern können.

Verwendete Technologien:

- **Heuristische Analyse**

  Die heuristische Analyse ist eine regelbasierende Scanmethode, die bestimmte Merkmale einer Mail erkennt. Bestimmte Merkmale deuten auf Spammails hin (z.b. wenn sich ein Removelink in dieser Mail befindet, bestimmte Wörter enthalten "VIAGRA", fremdsprachige Zeichensätze beinhalten etc..). Diesen Merkmalen werden unterschiedliche "Schlechtpunkte" zugeordnet. Nach der Analyse einer Mail werden diese "Schlechtpunkte" addiert. Wenn diese Summe über einem bestimmten Grenzwert liegt, wird diese Mail als Spam bewertet.

- **Bayes'sche Textanalyse**

  Die Bayes'sche Analyse greift auf Statistiken zurück, die auf das Analysieren von vielen Spammails entstanden sind. Dieser Mechanismus ist selbst lernend und wird mit der Anzahl von analysierten Mails intelligenter. Diese Statistiken werden mit algorithmischen Regelwerken auf neue Emails angewendet. Die Bayes'sche Analyse gilt als einer der stärksten Mechanismen in der Spamerkennung. Gleichzeitig auch als einer mit der geringsten "False positive" Rate. ("False Positives" sind reguläre Emails die als Spam beurteilt wurden - Je stärker ein heuristischer Spamfilter konfiguertiert wurde, desto höher ist die Rate von "False Positives") - Deshalb sind kombinierte Spamfilteringansätze sehr sinnvoll: D.h. Mails die mit einer sehr hohen Wahrscheinlichkeit als Spam bewertet wurden, können gleich gelöscht werden. Andere mit einer niedrigeren Spambewertung sollten nur markiert ("getagt") und nochmals vom Endbenutzer kontrolliert werden.

- **Lexikalische Analyse**

  Diese Analyseform untersucht den Inhalt der E-Mail und filtert Text-Strings (z.B. Verkaufsangebote, Aufforderung zum Besuch einer Webseite, etc.), Diese Textstrings werden mit Bool'schen Operatoren verknüpft (OR, AND, NOT etc.) und analysiert ob es sich tatsächlich um ein solches Angebot handeln könnte. Ist dieser der Fall wird das Emails als Spam qualifiziert.

- **Spamdatenbank**

  Spammails werden ab und zu geringfügig geändert (entweder mit jedem versandten Paket oder mit jeder versandten E-Mail). Um solche polymorphen Spammails zu identifizieren werden Hash-Signaturen aus empfangenen E-Mails extrahiert und mit Signaturen bekannter Spammails in einer aktualisierbaren Datenbank verglichen. Mit diesem Hash-Signatur-System lassen sich Variationen von Spammails erkennen.

  Die Filterung von verschiedenen Sonderzeichen, Daten und Tags, mit denen Spammails Antispamprogramme umgehen wollen, aus verdächtigen Spammails erhöht die Effektivität dieses Systems.

  Um die Datenbank aktuell zu halten werden Hash-Signaturen hinzugefügt, die mit Hilfe von sog. "Real-time Spam Collectors", E-Mail-Adressen die zum Sammeln von Spammails genutzt werden, erfasst werden.

- **Black- und Whitelists**

  Manchmal kann es jedoch notwendig sein, solche RBL-Listen zu spezifizieren. Diese Technik ist zwar veraltet, da Spammer sich zufällig E-Mail-Adressen von meist gültigen Domains auswählen und diese bei jedem Versand verändern. Dennoch werden immer noch bestimmte Domainnamen von Spammern benutzt um Spammails zu verschicken. Diese Domainnamen kann man selbst in Blacklists eintragen, um sich so vor Spam zu schützen.

  White Lists sind das Gegenstück zu Blacklists. In ihnen werden Listen von E-Mail-Adressen und Domains verwaltet, die erwünscht eine hohe Anzahl an Mails verschicken wie abonnierte Mailing-Listen oder Newsletter. Hier können auch E-Mail-Adressen hinzugefügt werden, die nicht von Spammern genutzt werden, aber zu einer Domain gehören, die gewöhnlich als Open Relay zum Versenden von Spammails missbraucht werden.

- **Subject Analyse**

  Viele Spammails ähneln sich in ihren Betreffzeilen. Durch Musterlisten, die typische Betreffzeilen von Spammails enthalten, ist es möglich Spam zu ermitteln und somit zu filtern. ("Save Money", "Viagra online",etc.)

- **Schutz vor Directory Harvesting-Attacken**

  Die so genannten Verzeichnis-Attacken werden von Spammern genutzt, um an gültige Email-Adressen einer Domain zu kommen. Dabei werden an viele verschiedene Adressen Mails verschickt und überprüft, ob der empfangende Mailserver eine Fehlermeldung zurückgibt. Ist dies nicht der Fall, ist die Email-Adresse gültig und wird in Spammailing Listen aufgenommen. Wird eine solche Directory Harvesting Attacke registriert, werden alle Emails dieses Senders geblockt.

- **Mailbombing Protection**

  Denial of Service (DoS)-Attaken sind eine Form des Mail-Bombing, bei denen versucht wird über Dictionary-Mailer Massen-E-Mails an eine Domain zu senden. Dieser Schutz reguliert den Email-Fluss um einer Überlastung vorzubeugen. D.h. Dass sowohl die Anzahl der offenen Email Sessions als auch die Anzahl der Emails im Spool überwacht werden.

  Eine beliebte Vorgehensweise von Spammern ist es, Emails mit einer großen

Anzahl von Empfängern zu verschicken. Dabei wird der Mailserver des Betroffenen als Multiplikator verwendet. Zum Schutz vor solchen Attacken ist beim IKARUS Spamfiltering ist eine maximale Höchstzahl an erlaubten Empfängern vordefiniert.

- **Relay Spoofing Protection**

  Spammer verschicken ihre Mails von externen Domains, verwenden aber zur Tarnung interne Absender-Adressen.

  Beispiele:

  - Eine Spammail an mike@yourcompany.com könnte sich im Absender als mikesfriend@yourcompany.com tarnen. Diese interne Absender-Adresse kann sowohl eine gültige als auch eine ungültige Adresse der Domain sein.

  - Als Absender-Adresse wird als Tarnung dieselbe Adresse wie die des Empfängers verwendet. Es scheint, als schicke man sich selber eine E-Mail.

  Emailspoofing wird von IKARUS Spamfiltering zuverlässig erkannt und unterbunden

Was ist ein IKARUS ScanCenter ?

Ein IKARUS ScanCenter ist eine zentral gehostete Infrastruktur in dem Antiviren- und Spamfilteringservices für Emails (IKARUS Managed Security Services), betrieben werden. Wahlweise kann der Serviceanbieter entscheiden, ob er ein eigenes "IKARUS ScanCenter" in seinem NOC betreiben will, oder das bestehende IKARUS ScanCenter das von IKARUS Software am VIX-2 in Wien gemanaged wird, nützen will.

Beschreibung IKARUS Scan Center:

Das IKARUS ScanCenter wird am VIX-2 (Interxion) in Wien gehostet, und von IKARUS Mitarbeiten 24x7 gewartet und überwacht.

Die Sicherheit wird durch geclusterte Firewalls gewährleistet. Die aktuelle Scanleistung ist derzeit für etwa 300.000 User ausgelegt. Diese Leistung kann im Bedarfsfall sehr einfach nach oben skaliert werden. Die Kommunikation im Scancenter erfolgt über physikalisch getrennte VLANs.

Die High Availability wird mit Hilfe von hot standby failovers gewährleistet. Das IKARUS Scan Center beruht auf Leading Edge Technologie

Technische Informationen:

Den IKARUS ScanCenter besteht aus:

- Firewalling
- Antivirenscanning
- Spamfiltering
- Datenbankenserver
- Webinterfaceserver
- Wartungsserver

(diese Funktionen sind selbstverständlich redundant und skalierbar ausgelegt!)

Verwendete Technologien:

- High Availability mit Hot Standby Failover
- GNU basiertes Loadbalancing
- Heartbeat Monitoring
- separates Wartungs-LAN
- Firewall Cluster
- physikalisch getrennte VLANs
- gehärtete Betriebsysteme

Betriebsysteme:

Linux und Windows 2000 Server.
Datenbank: SQL

Update-Zyklen

Das IKARUS Scan Center wird via Push-Strategie mit den aktuellen Virendatenbank-Files, Scanner-Updates und Spamfilteringrules versorgt. Die Übertragung der Dateien erfolgt verschlüsselt über SMTP.

Installation / Enabling

Die Lösung wird vorinstalliert auf "Secureguard" - Servern geliefert und zusammen mit technischem Personal des IKARUS MSS Serviceproviders in Betrieb genommen.
Wartung und Konfiguration obliegt dem IKARUS MSS Serviceprovider und IKARUS Software.

Entscheidet sich der Serviceanbieter dazu Servicereselling zu betreiben, und nützt dabei die Infrastruktur von IKARUS Software, ist kein Aufwand erforderlich.

Gegenüberstellung der Kosten:

dediziertes Unternehmensgateway / IKARUS Managed Security Services

Aufwendungen	**Gateway**	**IKARUS ScanCenter**
Planung/Evaluierung	2 Mann-Wochen € 2.000	2 Mann-Wochen € 2.000
Hardware-Anschaffungen	€ 2.000	€ 0

Software Lizenzkosten für Virenschutz/Spamfilter	€ 2.300	€ 3.100
Installation/Konfiguration/Roll-out	1 Mann-Woche € 1.000	1 Mann-Stunde € 100
Laufende Wartungskosten, Anpassungen/Jahr	3 Tage/Monat € 5.800	€ 900
GESAMT	**€ 13.100,--**	**€ 6.100,--**
(Basis: Unternehmen mit 100 Usern Kosten/Jahr) **ERSPARNIS: € 7.000,--**		

Die Preise für **IKARUS myM@ilWall** werden pro User (Anzahl der Mitarbeiter die einen Internetzugang im Unternehmen besitzen) und Laufzeit(Jahre) berechnet. Supportpreise beinhalten Konfigurationssupport und Telefonsupport bei aktuellen Virenproblemen etc.

Berechungsbeispiele:

1. Useranzahl: bis 300; Laufzeit: 2 Jahre; mit Support = (6.647 + 1.899)x2 (Jahre) = **17.092 Euro** (professional)

2. Useranzahl: bis 50; Laufzeit: 1 Jahr; ohne Support = **1.703 Euro**

Preiskalkulation:

Verwenden Sie bequem und schnell unseren Preiskalkulator.

Preiskalkulator für IKARUS myM@ilWall professional. (Virenschutz + Spam-Filtering)

Sollte der **IKARUS myM@ilWall** Preiskalkulator nicht funktioneren, haben Sie eventuell JavaScript nicht installiert oder deaktiviert. Sie können jedoch unsere **kompletten Preislisten** ansehen und ausdrucken.

Preisliste für für IKARUS myM@ilWall professional. (Virenschutz + Spam-Filtering)

Hinweis:
Diese Preise gelten nur für Kunden, die **IKARUS MANAGED SECURITY SERVICES** über **IKARUS Scan Center** beziehen. Die Preise werden wie bei Softwarelizenzen auf Basis von Userzahlen berechnet.

Die SLA für **IKARUS MANAGED SECURITY SERVICES** können Sie **hier** herunterladen.

Millionen von Emails werden in den IKARUS Scan Centern zum Schutz vor Computerviren und Spam bearbeitet. Um dem Vertrauen, dass dabei 1000de Firmen in uns setzen gerecht zu werden, wollen wir hier nochmals mit Nachdruck erwähnen dass:

Die IKARUS Software GmbH und deren Mitarbeiter der Schweigepflicht des Fernmeldegesetzes und den Geheimhalteverpflichtungen des Datenschutzgesetzes unterliegen. Dazu gehört unter anderem, dass über das technisch notwendige Mindestmaß keine Inhaltsdaten gespeichert und keinesfalls ausgewertet werden. Zusätzlich schützt eine interne Information Security Policy den vertraulichen Umgang mit Ihren Daten.

Ihre Daten werden nicht nur durch Gesetze geschützt, sondern auch durch physische Maßnahmen gesichert:

- Redundante Systemauslegung und hochverfügbare Firewalls
- Ausfallssichere Stromversorgung durch USV-Anlagen und Backup-Generatoren
- 24 x 7 x 365 Zugangskontrolle und Bewachung
- Brandmelde- und Brandlöschanlagen
- Redundante Klimakontroll- und Kühlsysteme

Zufriedene Kunden und ISPs über IKARUS Managed Security Services:

VIATRIS Pharma GmbH:

IKARUS Managed Security Services bedeuten für mich eine ungemeine Arbeitserleichterung, da ich mich nicht mehr um die Wartung bemühen muss. Ich bin mir sicher, dass immer die aktuellste Virendatenbank aktiv ist.
Einmal richtig konfiguriert ist meine Arbeit getan und Ikarus Software kümmert sich um die laufenden Wartungsarbeiten. Außerdem habe ich bei Fragen oder Problemen in Ikarus Software einen kompetenten und rasch reagierenden Partner gefunden.

Andreas Förster
EDV Netzwerkorganisation

TELEKOM Austria:

Telekom Austria hält permanent Ausschau nach neuen Produkten, für die der Kunde bereit ist zu zahlen. So haben wir entschieden, ein Virenschutz- und Spamfilteringsystem zu realisieren daß stabil, hochperformant uns skalierbar ist. Aber auch andere Punkte mußten erfüllt werden: Clustering, Loadbalancing, eine existierende Authentifizierung,
Mandantenfähigkeit, sowie die Intergrierbarkeit in ein bestehendes Mailsystem. Für dieses wichtige Projekt wollten wir ausschließlich mit einem Partner arbeiten, der bereits Erfahrung im ISP Business hat, und auf einer stabilen finanziellen Basis steht. Mit IKARUS Software und deren Produkt IKARUS Managed Security Services haben wir den idealen Partner gefunden. Nach den ersten beiden aktiven Monaten, waren wir sicher die richtige Entscheidung getroffen zu haben: Das System arbeitet technisch perfekt, und wir haben bereits unsere Umsatzerwartungen übertreffen können.

Christian Schubert
Product Management Telekom Austria

Tiscali AG :

Die Tiscali AG ist ein ISP mit Fokus auf Datensicherheit, und bietet deshalb seinen Kunden ausschließlich hochqualitative Produkte für diesen Bereich. Mit IKARUS Managed Security Services haben wir ein Produkt gefunden, das unsere hochwertige Produktpalette ideal ergänzt.

Helmut Michel,
Security Engineer Tiscali AG

Einige Fragen die uns bereits gestellt wurden:

- Ich habe bereits Virenschutz im Einsatz, soll ich IKARUS Managed Security Services trotzdem verwenden?
- Welche Zusatzfeatures bietet IKARUS Managed Security Services?
- Werden meine E-Mails gemäß Datenschutzgesetzen behandelt?
- Welche Firmen können das Service von IKARUS Managed Security Services subscriben?
- Was passiert mit infizierten Emails?
- Erkennt IKARUS Managed Security Services unbekannte Computerviren?
- Was passiert, wenn ein Computervirus gefunden, aber nicht entfernt werden kann?

- Wie werde ich vor High Outbreaks (z.B. Loveletter, Sobig, Sasser etc.) geschützt?
- Wo passiert das Virenscanning?
- Wie oft werden die Virendatenbanken upgedated?
- Von wem kann IKARUS Managed Security Services konfiguriert werden?
- Gibt es Verzögerungen beim Empfang bzw.Versand von E-Mails?
- Welchen Aufwand habe ich als Kunde?
- Wie funktioniert der E-Mailtraffic mit IKARUS Managed Security Services?
- Erkennt IKARUS Managed Security Services auch Mehrwertdialer?

Ich habe bereits Virenschutz im Einsatz, soll ich IKARUS Managed Security Services trotzdem verwenden?

Ja, auf jeden Fall, da IKARUS Managed Security Services

- als 2. Virenscanner die Sicherheit zusätzlich erhöht. (4 Augen sehen mehr als 2!)
- via Push-Update stets mit den aktuellsten Virendatenbanken ausgestattet wird, 24 Stunden/
  7 Tage in der Woche. Im Regelfall ist eine Push-Update-Strategie um bis zu einer Stunde schneller als ein Pullupdate (Ein Antivirenprogramm überprüft im Normalfall einmal pro Stunde ob ein neues Update verfügbar ist). Bei der Push-Update-Strategie wird die IKARUS Managed Security Services upgedatet sobald IKARUS ein neues Update verfügbar hat - also sofort.
- Viren bereits abfängt bevor sie die technische Infrastruktur Ihres Unternehmens erreichen ("First line of Defence" - Prinzip)

oben

Welche Zusatzfeatures bietet IKARUS Managed Security Services?

Die sind:

- Virenschutz
- Messaging
- Anlagenfilter
- Protokolle und Statistiken
- Spamfiltering

oben

Werden meine E-Mails gemäß Datenschutzgesetzen behandelt?

Wie alle Online- und Access Services unterliegt auch der Virenschutz und das Spamfiltering durch IKARUS Managed Security Services den Datenschutzgesetzen.

oben

Welche Firmen können das Service von IKARUS Managed Security Services subscriben?

Für alle Personen/Firmen, die im Besitz einer eigenen Domain sind.

oben

Was passiert mit infizierten Emails?

1. Virus wird erkannt und abhängig von der Konfiguration aus Email/Anlage entfernt.
2. Bei Verwendung einer Quarantäne-Mailbox geht der virale Inhalt gepackt und verschlüsselt an die
   Administrator-Adresse.
3. Je nach Konfiguration wird eine Warnung an den Absender/Empfänger des verseuchten Emails
   geschickt.
4. Das vom Virus befreite Email wird zugestellt.

oben

Erkennt IKARUS Managed Security Services unbekannte Computerviren?

IKARUS Manaegd Security Services verwendet 3 verschiedene Scanmethoden:

Patternscanner, Heuristischer Scanner und eine spezielle Heuristik für Scripts. Mit heuristischen Methoden ist es auch möglich auch möglich unbekannte Viren zu erkennen.

1) Der Patternscanner erkennt Computerviren aufgrund ihrer charakteristischen Bitstruktur (Aussehen).
d.h.. Der Antivirenprogrammierer benötigt zuerst den Virus selbst - damit er ein "Gegenmittel" entwickeln kann.

2) Als Heuristischen Scanner bezeichnet man ein Programm, das einen virtuellen Computer simuliert und selbständig Programme analysiert. Mit dieser Technik erkennt der heuristische Scanner Computerviren aufgrund ihres Verhaltens. D.h.: Auch unbekannte Computerviren werden gefunden!

oben

Was passiert, wenn ein Computervirus gefunden, aber nicht entfernt werden kann?

Das Email bzw. die Anlage wird in diesem Fall gelöscht, an Empfänger und Absender geht eine Verständigung. Die Quarantäne-Funktion verhindert hierbei, dass Inhalte unwiederbringlich verloren gehen. Das Email wird anschließend gepackt und verschlüsselt an die Administrator-Mailbox zugestellt.

oben

Wie werde ich vor High Outbreaks (z.B. Loveletter, Sobig, Sasser etc.) geschützt?

Durch Statistiken und Online-Regelwerke werden Trafficanomalien (Unregelmäßigkeiten im Emailverkehr) erkannt und diese an Virenanalytiker weitergemeldet, die ihrerseits die notwendigen Schritte einleiten, um Sie zu schützen.

Zusätzlich arbeitet IKARUS Software in Bezug auf das Austauschen von neuen Viren-Samples mit anderen internationalen AV-Softwareherstellern zusammen (z.B. REVS - rapid exchange of virus-samples).

oben

Wo passiert das Virenscanning?

Direkt im IKARUS Scan Center im zentral gehosteten Datencenter.

oben

Wie oft werden die Virendatenbanken upgedated?

Normalerweise täglich. Im Bedarfsfall (bei High Outbreaks) öfter.

oben

Von wem kann IKARUS Managed Security Services konfiguriert werden?

- Vom User über das Benutzerinterface.
- Zu Supportzwecken direkt von IKARUS Software über ein eigenes Administrator-Interface.

oben

Gibt es Verzögerungen beim Empfang bzw.Versand von E-Mails?

Durch die Verwendung von IKARUS Managed Security Services kommt es zu keinen für den User spürbaren Performance-Einbußen beim Email-Verkehr.

oben

Welchen Aufwand habe ich als Kunde?

So gut wie keinen! Einfach registrieren, die Bestätigung des Antrages zur Änderung des MX-Eintrages (den Sie von uns erhalten) an Ihren Provider weiterschicken. - Wir schalten sie dann auf - und schon sind Sie sicher!

oben

Wie funktioniert der E-Mailtraffic mit IKARUS Managed Security Services?

Siehe Grafik.

Erkennt IKARUS Managed Security Services auch Mehrwertdialer?

Ja. IKARUS Managed Security Services erkennen beinahe 100% aller im Umlauf befindlichen Mehrwertdialer.