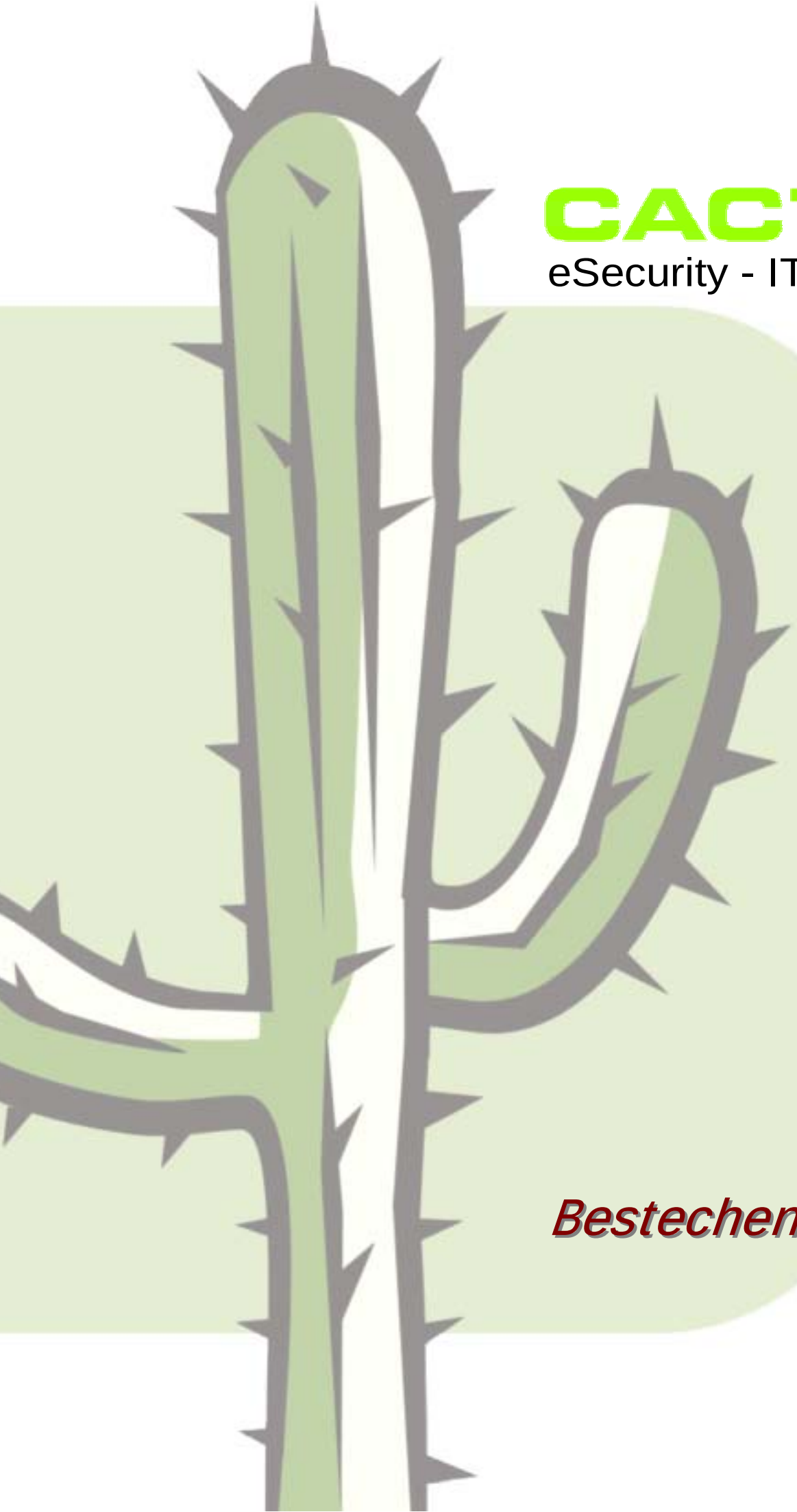


CACTUS

eSecurity - IT-Sicherheit

Bestechend sicher!

Die Risiken werden vielfältiger

Wer Firewall und Virenschutz einsetzt, ist heute nicht mehr automatisch auf der sicheren Seite!

Viren, Würmer, Spam

Computer und Netzwerke sind einer ständig zunehmenden Bedrohung ausgesetzt. Potenzielle Gefahrenquellen sind neben Zugriffen auf interne Daten auch Sabotage oder Datendiebstahl, beispielsweise ausgeführt durch Insider. Viele Angriffe finden heute auf der Anwendungsebene statt und können damit traditionelle Firewallsysteme ungehindert passieren.

Störung geschäftskritischer IT

In den heute weitgehend von IT-Systemen abhängigen Unternehmensprozessen haben Schadensfälle geschäftskritische Wirkung. Der gesamte Unternehmensablauf oder Teile davon (Einkauf, Produktion, Vertrieb) können derart gestört sein, dass es nicht nur zu Ausfällen kommt, sondern der Fortbestand des Unternehmens gefährdet sein kann.

Sinkende Produktivität

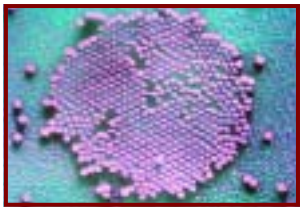
Die Topkonzerne der USA werden nur durch Spam-Mails allein im Jahr 2004 mit Kosten von 1934 Dollar pro Mitarbeiter konfrontiert sein. Damit, so ergab eine Studie des amerikanischen Forschungs-institutes Nucleus Research, hat sich der Wert gegenüber dem Vorjahr mehr als verdoppelt (874 Dollar). Durchschnittlich erhalten die Angestellten der Studie zu-folge 29 unerwünschte E-Mails pro Arbeitstag, gegenüber 13 im Vorjahr.

Imageschädigung

Oft ist die Imageschädigung das größte Problem: Wenn etwa eine Bank ihren Kunden die sichere Aufbewahrung des Vermögens als Dienstleistung verkauft, die eigenen IT-Systeme aber so unzureichend schützt, dass es Hackern gelingt, den Inhalt des Webservers der Bank zu verändern (so genanntes Defacement), sinkt das Vertrauen der Kunden rapide.

Unternehmensranking

Dass die Gefahren ernst zu nehmen sind, ist auch daran zu messen, dass die Güte der IT-Sicherheit eines Unternehmens zunehmend in das Rating nach Basel II einbezogen wird.



Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) sollte bei der Planung der IT eines Unternehmens auch berücksichtigt werden.

Was Kunden über uns sagen:

"CACTUS eSecurity unterstützt uns schon lange kompetent im Bereich Netzwerksicherheit"

Dipl.-Ing. Meik Hilfrich
Leiter Internet & Network-Security Integrated Network Products
Lufthansa Systems

Ralf Hayn
Geschäftsführender Gesellschafter
Spezialist für technische IT-Sicherheit

Tim Purschke
Geschäftsführender Gesellschafter
Experte für organisatorische Sicherheit

CACTUS eSecurity: Wir über uns

Anfang 1999 gründeten wir die CACTUS eSecurity GmbH in Frankfurt am Main. Unsere Wurzeln liegen im Firewalling-Umfeld. Leistungsspektrum und Teamgröße wuchsen jedoch schnell, so dass wir heute zu den Spezialisten mit sehr umfangreicher und tief gehender Erfahrung in allen wichtigen Bereichen der IT-Sicherheit zählen.

Je nach Projektgröße und inhaltlicher Anforderung arbeiten wir neben dem festen Mitarbeiterteam mit einer Reihe freier Spezialisten zusammen. Gemeinsam bilden wir ein Netzwerk, das für seine hohe Spezialisierung in der IT-Sicherheit bekannt ist.

Kunden schätzen unsere Flexibilität, die durch unsere Produktunabhängigkeit noch verstärkt wird, sowie unsere individuell zugeschnittene Beratung. Zu unseren Kunden zählen u. a. Systemhäuser, Banken, Behörden und Firmen aus der Logistik- und Touristik-Branche.

Unser Portfolio reicht von der Beratung über die Konzeptionserstellung bis zum technischen Support, der Ihnen bei Bedarf 7 x 24 h zur Verfügung steht. Selbstverständlich erstellen wir zu allen Projektphasen eine ausführliche Dokumentation und schulen Ihre

Der „Cactus", wehrhaftes Symbol für unseren Arbeitsfokus

Weitere Informationen:

CACTUS eSecurity GmbH
Adolf-Reichwein-Straße 1
60320 Frankfurt am Main

Sandbergstraße 14
64285 Darmstadt

Telefon 069 - 61 99 59 82
eMail: info@cactus.de
http://www.cactus.de

Was Kunden über uns sagen:

"Da ein Großteil unserer Kunden aus dem Finanzsektor stammt und besondere Ansprüche an den Themenkomplex Sicherheit in der IT stellt, sind wir froh, mit der Firma CACTUS eSecurity einen kompetenten Partner bei der Planung, Implementierung und Betriebsführung dieses komplexen und äußerst sensiblen Produktportfolios gefunden zu haben."

Matthias Tauber
Referatsleiter IT-Sicherheits- und Internet Services
IZB Informatik-Zentrum München-Frankfurt a. M. GmbH & Co. KG

Die 8 CACTUS-Kompetenzen

Unsere Kernkompetenzen präsentieren wir Ihnen in acht Komponenten:

1. Organisatorische Sicherheit
2. Sicherheitsanalyse
3. Systemsicherheit
4. Netzwerkabsicherung
5. Authentisierung
6. Wahrung der Vertraulichkeit
7. Ausfallsicherheit
8. Alarmierung und Reaktion

Diese Spezialisierung in Verbindung mit vielen Jahren Erfahrung zeichnet uns aus.

1 Organisatorische Sicherheit

Wir helfen Ihnen bei der Erstellung umfassender, lückenloser Sicherheits-konzepte.

Auf Grund von Analyse und Risikoabschätzung erstellen wir die für Ihr Unternehmen maßgeschneiderte Lösungsstrategie in Form eines ISO 17799-basierten Sicherheitskonzeptes.

Dabei berücksichtigen wir sowohl die technischen als auch die organisatorischen Belange, etwa in Form von sicherheitsrelevanten Arbeitsprozessen.

Bei der Erstellung Ihrer globalen Sicherheitsrichtlinien (Security Policy) sind wir Ihnen gern behilflich.

Unser Portfolio reicht dabei von der allgemeinen Schärfung des Sicherheitsbewusstseins bis hin zu produkt-spezifischen Schulungen für eine Vielzahl von Sicherheitslösungen.

2 Sicherheitsanalyse

Die Identifizierung der vorhandenen Schwachstellen ist der erste Schritt. Hierbei berücksichtigen wir sowohl die technische Sicherheit der gesamten Unternehmens-IT-Infrastruktur als auch organisatorische Maßnahmen.

Diese Überprüfung erfolgt nach dem „Open Source Security Testing Methodology Manual“ (OSSTMM).

Dabei werden alle Prozesse der Informationssicherheit, die gelebte Sicherheit der Mitarbeiter („Social Engineering“) sowie die Schwachstellen der IT-Systeme im technischen Teil mittels “Penetra-tions-Tests“ beleuchtet.

Besonders diese ganzheit-liche Vorgehensweise hat sich in der Vergangenheit als

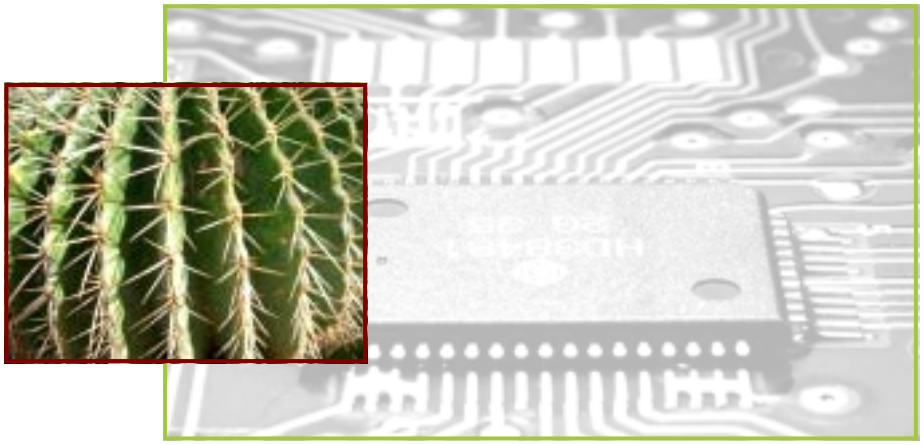
3 Systemsicherheit

Wir erhöhen die Sicherheit Ihrer IT-Systeme durch individuelles System-Hardening für Windows- und Unix-Server ebenso wie für Netzwerkkomponenten (Router, Switch, Loadbalancer, Firewall). Dabei minimieren wir die Angriffsfläche Ihrer Systeme für potenzielle Angreifer.

Das Schließen neu auftauchender Sicherheitslücken ist zur dauerhaften Erhaltung der Systemsicherheit von zentraler Bedeutung.

Etablierung und Schulung eines CERT (Computer Emergency Response Team) sowie funktionierendes Patch-Management sind Voraussetzungen für zeitnahe und reibungslos funktionierende Gegenmaßnahmen. Bei all dem können wir Sie unterstützen oder Teilaufgaben komplett übernehmen, indem wir Ihnen z. B. individuell notwendige Sicherheits-informationen liefern.

Auch die Sicherheit der Arbeitsplatzrechner darf nicht zu kurz kommen: Wir arbeiten nach den im IT Grundschutz-Handbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI)



Den hohen Sicherheitsstandard unserer Kunden erreichen wir durch den Einsatz folgender Werkzeuge:

Firewallsysteme:
Symantec Enterprise Firewall, Juniper Netscreen, Intermate TrustGate, Check Point, phion, iptables

Authentisierungssysteme:
SecureComputing Safeword, RSA ACE Server, Vasco Digipass, Entrust Authority PKI

VPN-Lösungen:
Juniper Netscreen (SA), Infotecs ViPNet, Datafellows, Check Point, ssh, FreeS/WAN

Hochverfügbarkeitslösungen:
Rainfinity Rainwall, Nortel Alteon, Stonesoft, Cisco

Network Security Scanner:
Nessus, ISS, Retina, QualisGuard, Nmap

Intrusion Detection Systeme:
ISS RealSecure, SiteProtector, Juniper

4 Netzwerk-absicherung

Unsere Kernkompetenz liegt in der Absicherung Ihrer netzwerkbasierten Kommunikation. Firewalling, Screening-Router, VLAN-Separierung, VPN, Security-Proxies und sichere Internet-Dienste (DNS, HTTP, eMail) - wir unterstützen Sie in allen Bereichen und in allen Projekt-phasen (Planung, Implementierung, Betriebsführung).

Firewalls sind seit deren Markteinführung unser Geschäft, von einfachen Paketfiltern über Stateful-Firewall-Systeme und Application-Level-Gateways bis zu mehrstufigen, hochverfüg-baren Firewall-Lösungen - wir sind für jede Ausbaustufe der richtige und

CACTUS eSecurity : Kontrollierter Zugang zu Ihren Datenbanken, Ihrer eBusiness-Umgebung oder dem SAP-Umfeld

5 Authentisierung

Um sicher zu sein, dass eine Person wirklich berechtigt ist, den von Ihnen angebotenen IT Dienst zu nutzen, bedarf es adäquater Authentisierungssysteme.

Für den Zugriff auf kritische Unternehmensbereiche empfehlen wir die Verwendung einer 2-Faktor-Authentisierung.

Bei dieser, auch als „starke Authentisierung“ bezeichneten Variante kann sich ein Benutzer nur erfolgreich ausweisen, wenn er über zwei separate Merkmale verfügt, etwa „Wissen“ in Form eines Passwortes und „Besitz“ in Form eines Hardware-Tokens oder einer SmartCard.

Auch auf dem Gebiet der Public Key Infrastructure (PKI) unterstützen wir Sie bei der Einrichtung einer individuell angepassten Authentisierungslösung.

PKI bezeichnet eine technische **und** organisatorische Infrastruktur, welche die Verwaltung von Schlüsseln und zugehörigen Zertifikaten ermöglicht.

6 Wahrung der Vertraulichkeit

Die Bedrohung der IT durch unberechtigte Zugriffe wird leicht unterschätzt:
Triviale Zwischenfälle wie entwendete oder verlorene Laptops bringen Unternehmen oder auch Behörden in peinliche und Image-schädigende Situationen.
Werden vertrauliche, personenbezogene Daten bekannt, drohen rechtliche Konsequenzen.

Geeignete Verschlüsselungsmechanismen, sowohl bei der Speicherung der Daten als auch bei der Kommunikation zwischen IT-Systemen, verringern die Gefahren deutlich. Hierbei kommen unter anderem die Protokolle IPSec, SSH, SSL und TLS zum Einsatz.

Wir unterstützen Sie bei der Konzeption zur Absicherung Ihrer Daten und bei der Auswahl und Implementierung der für Ihre

7 Ausfallsicherheit

Ein IT-Dienst Ihres Unternehmens muss jederzeit für Ihre Kunden erreichbar sein? Dann muss neben dem Server-System, das den Dienst bereitstellt, auch die Infrastruktur bis zu diesem System hochverfügbar ausgelegt werden.

Hier empfiehlt sich ein redundanter Aufbau aller Systeme, die sich im kritischen Pfad der Kommunikation befinden.

Wir bieten Lösungen zur Steigerung der Verfügbarkeit von Routern, Switches, Firewalls und Server-Systemen, vom einfachen Bereithalten eines identisch konfigurierten Ersatzsystems (cold standby) bis zu hochverfügbaren Clustern mit dem gleichzeitigen Betrieb mehrerer Einzeleinheiten (Load-Balancing-Verfahren).

8 Alarmierung und Reaktion

Frühzeitige Erkennung von Angriffen erfordert permanente Überwachung der existierenden Sicherheitssysteme. Selbst bei personal-intensiver 24-Stunden-Überwachung verhindern große Datenmengen, alle Angriffe zeitnah zu analysieren.
Dieses Problem lösen wir mit unterschiedlichen, sich teilweise ergänzenden, technischen Lösungen:

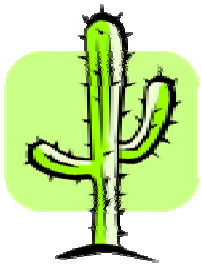
- Systeme zur automatisierten Logfile-Analyse, die dazu dienen, große Datenmengen sinnvoll zu filtern und die Auswertung zu vereinfachen.
- Intrusion Detection Systeme, kurz: IDS, die in der Lage sind, Angriffe in Echtzeit zu erkennen und entsprechende Alarmierungen auf unterschiedlichen Wegen zu generieren.
- Intrusion Prevention Systeme, kurz „IPS“, die erkannte Angriffe automatisch blockieren.

Automatisierte Reaktion verlangt ein sorgfältig erarbeitetes Konzept, damit gewollte Kommunikation nicht verhindert wird. Zusätzlich wird ein Plan benötigt, in welchem das Vorgehen im Fall eines Angriffs beschrieben wird.

Wir unterstützen Sie bei der Erstellung entsprechender Handlungsanweisungen (Incident Handling) und beim Aufbau eines eigenes CERT (Computer Emergency Response Team).

So kann Ihr Unternehmen

Mit CACTUS eSecurity Risiken erkennen und beseitigen!



CACTUS eSecurity GmbH

Adolf-Reichwein-Straße 1
60320 Frankfurt am Main

Sandbergstraße 14
64285 Darmstadt

Telefon 069 - 61 99 59 82
Telefax 069 - 61 99 59 84

eMail info@cactus.de
http://www.cactus.de