



## Security Breakfast:

# Secure Hosting - was heißt das in der Praxis?

Veranstaltung

11. Juni 2010

Referent

Ulrich Gärtner

Leiter Vertrieb

Pallas GmbH  
Hermülheimer Straße 10  
50321 Brühl

information(at)pallas.de  
<http://www.pallas.de>





## Professionelle Infrastruktur + Service

Serverbetreiber	Websitebetreiber	Nutzer
Server härten	Sichere Softwarearchitektur und sichere Programmierung	Virenschutz frisch halten
Firewall vorschalten	Fremdprogramme aktuell halten	URL-Filter zwischenschalten
Auf Schadsoftware prüfen	Web Application Firewall vorschalten	Browser und wichtige Programme aktuell halten



- Klima + Unterbrechungsfreier Strom
- Brandschutz
- Zugangsschutz
  - Zugangsschutz zum RZ
  - Zugangsschutz zum Backup
- Je nach Verfügbarkeitsanforderungen
  - Zwei Brandschutzzonen
  - Ausweich RZ für Katastrophenfall
- Internet Uplink
  - Redundant über mehrere Provider (eigenes AS)
  - Bandbreitenreserve für Lastspitzen



- Firewall vorschalten
  - Redundant
  - Minimal-Policy
  
- Zonen bilden nach Kritizität
  - der Zugriffsrechte des Kunden
  - der Anwendungen / Skripte



- Web 2.0 fordert Bereitstellung bisheriger Intranet-Anwendungen auch im Web
- Zielscheibe für kriminelle Angriffe wie SQL-Injection, Cross-Site Scripting und Denial-of-Service (DOS)
- Lösung: Web Application Firewall (WAF) vorschalten



- Funktionsweise:
  - Die WAF untersucht alle eingehenden Anfragen und die Antworten des Web-Servers. Bei verdächtigen Inhalten wird der Zugriff unterbunden. Generell wird nach dem Whitelist-Prinzip gearbeitet: Alles was nicht explizit erlaubt wird, ist verboten
  - Bei SSL-verschlüsseltem Datenverkehr (https) wird mittels SSL-Offloading der Datenverkehr entschlüsselt und geprüft
  
- Lernprozess:
  - WAF-Regelwerk wird mittels adaptiven Lernens (halb) automatisch erstellt.
  - In einer Lernphase wird die gesamte Anwendung vollständig in allen möglichen Varianten vom Nutzer verwendet
  - Der Lernprozess wird bei Aktualisierung der Anwendung erneut durchgeführt



- Server Hardware
  - Redundant
  - Kritische Bauteile überwachen
    - Netzteile, Festplatten, Lüfter
  - Austausch vor zu erwartendem Ausfall
- Server härten
  - OS härten: Nur notwendige Dienste werden aktiviert
  - Web-Server: Keine Verwendung unsicherer Module bzw. nur mit Einverständnis des Kunden
- Server Know-How
  - Eigenes Personal für Hardware-Wartung
  - Hersteller Wartungsverträge für komplizierte Fälle



- Mehrgenerationen Backup
  - Sicherungsumfang
    - Bei Pallas komplett mit Ausschluß von wenigen Verzeichnissen (z.B. /tmp) oder nicht sicherungswürdigen Massendaten
  - Sicherung täglich
  - Aufbewahrung je nach Anforderung
    - Bei Pallas ist 1 Jahr Standard
- Restore üben!
  - Einzeldateien, konsistente Sätze, Disaster-Recovery
- Katastrophenfall Absicherung
  - Auslagerung von Komplettsicherungen
  - Ggf. Spiegelung des Datenbestandes im Ausweich RZ



- Schadsoftware eliminieren
  - Webserver regelmäßig auf Inhalte mit Schadsoftware prüfen
  
- Fremdprogramme aktuell halten
  - Bei verfügbaren neuen Releases
  - Relevanz für den Kunden absprechen
  - Sicherheitskritische Releases werden i. d. Regel sofort eingespielt oder
  - Wenn möglich, wird vor Aufspielen auf das Produktivsystem auf einem Testsystem das Release getestet



- Überwachung
  - Erreichbarkeit der Server prüfen
  - Erreichbarkeit der Dienste auf dem Server
  - Überwachung der Internetanbindung, Plattenauslastungen, RAM, CPU
  - Bandbreitennutzung



- Alarmierung des Helpdesk
  - Direktansprache von Technikern
  - Fokus Geschäftskunden
    - Helpdesk von 9:00-18:00
- Alarmierung der Rufbereitschaft
  - 24x7 Rufbereitschaft
  - Alarmierung durch die Überwachung
  - Optional Direktdurchwahl durch den Kunden zur Rufbereitschaft



Gerne beantworte  
ich Ihre Fragen



Ulrich Gärtner, Leiter Vertrieb  
Pallas GmbH  
Hermülheimer Straße 10  
50321 Brühl

02232-1896-24  
ulrich.gaertner (at) pallas.de  
<http://www.pallas.de>



---

# Nächstes **Pallas Security Breakfast**

am Freitag den 24.09.2010, 9:00 Uhr