Novell/SUSE Security Team

Ein Einblick in Aufgaben und tägliche Arbeit

Marcus Meißner
SUSE Security Team Lead
meissner@suse.de
marcus@jet.franken.de

November 20, 2005

Novell®

SUSE Security Team

- Aufgehängt in der SUSE Entwicklung in Nürnberg
- 4 Mitglieder im Team
- Arbeitsbereich: Linux basierte Produkte von Novell
- Aufgaben:
  - Sicherheitsupdates für releaste Produkte
  - Security Reviews für zukünftige Produkte
  - Security relevante weitere Projekte
  - Forschung
- Sicherheit ist ein Prozess – kein Feature

Security Betreuung vor Release

- Technologien zum Erkennen von Problemen
  - Erkennen unsicherer Dateirechte (schreibbar für Welt, setuid)
  - Ersetzen von setuid Bits durch Technologien, die diese nicht brauchen: resource manager, ACLs, utempter
  - GCC Fortify Source – leichtgewichtige Tests auf Buffer overflow
  - GCC Stack Protector – nicht ganz so leichtgewichtige Tests
- Review des Sourcecodes von neuen Daemonen und Technologien
- Review des Designs von sicherheitsrelevanter Technologien (DBUS)

Security Projekt – Zertifizierung

- CCAPP/EAL2/3/4+ Projekte
  - Sicherheitszertifizierung zusammen mit dem BSI
  - Beschrieben für bestimmte Konfigurationen:
    - Annahmen in Bezug auf Angriffsszenarien
    - festgelegte Software und Versionen
    - festgelegte zertifizierte Hardware
    - festgelegte Konfiguration des Systems (PAM etc.)
  - Zertifikation stellt Auflagen an:
    - Sicherheitsprozesse
    - Software Produktionsprozesses
    - physikalische Sicherheit bei der Entwicklung
    - Dokumentation

Security – AppArmor/SubDomain

- Applikationen einsperren
- Zugriff auf Dateien einschränken per Whitelist
  - Schreib / Lesezugriff getrennt konfigurierbar
  - reguläre Ausdrücke / Wildcards
- Starten von Programmen verhindern
  - ntpd braucht kein Programm zu starten (z.B.)
- POSIX Capabilities
  - Apache braucht keine IO ports zu ändern
- Light Version auf der SUSE Linux 10.0

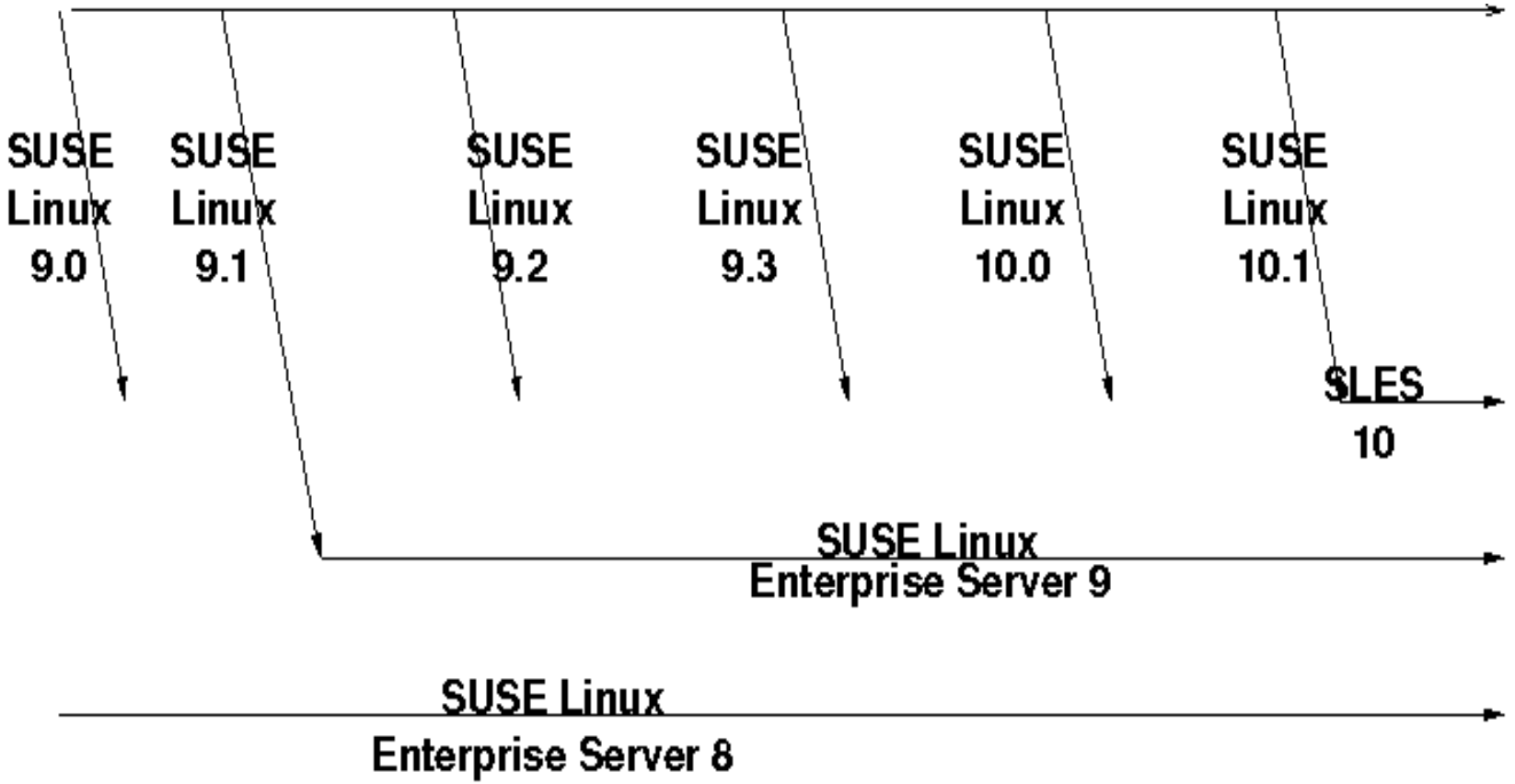
Sicherheitsprobleme im Lauf der Zeit

- Buffer overflows
- Formatstring Probleme
- Integer Überlauf -> wieder Buffer overflows
- Letztes und dieses Jahr:
  - Bild verarbeitende Bibliotheken
  - Probleme in Web Applikationen (meist PHP)
- Nächstes Jahr: ?
- Problem:
  - Immer mehr Code bearbeitet Daten aus dem Internet
  - Applikationen werden größer und größer

Produktlinien - Übersicht

- Retail / Heimanwender Produktlinie
  - Produkt: SUSE Linux (Professional) / openSUSE
  - Release: alle 6 Monate, Securitysupport für 2 Jahre
  - Je 4 bis 5 SUSE Linux Versionen jederzeit supported
  - Updates für Sicherheitsprobleme, kritische Fehler
- Enterprise Produktlinie
  - Produkte: SUSE Linux Enterprise Server, Novell Linux Desktop, Open Enterprise Server
  - Supportdauer: 5 Jahre (erweitert 7 Jahre)
  - Updates für Sicherheitsprobleme, Fehler, neue Hardwareunterstützung

Produktlinien - Vererbung



Produktlinien – Details

- Für jedes Produkt:
  - seperate Repositories für Sourcen
  - seperate Repositories für Binärpakete
    - pro Architektur (i386 , x86_64, ppc, ppc64, s390, s390x, ia64)
- Produkte bauen sich selber (in chroot Umgebungen)

Sicherheitsupdates & Paketversionen

Sicherheitsupdates:

- Dürfen keine Abhängigkeiten innerhalb des Systems verändern
- Keine Überraschungen für Administratoren

Deshalb:

- Pakete bleiben auf alter Version
- Patches werden hinzugefügt
- Erkennbar durch RPM Changelog (rpm -q –changelog paketname)

Sicherheitsupdates

- Hauptarbeit des Security Teams
- Informationen erreichen uns:
  - aus Mailinglisten (bugtraq, full-disclosure,...)
  - durch neue Software Releases
  - direkter Bericht an uns via security@suse.de oder Bugzilla
  - eigene Security Audits
- Evaluierung
  - sind wir betroffen?
- Tracking
  - via Bugzilla (http://bugzilla.novell.com)

Sicherheitsupdates - Bugzilla

- Bugzilla ist das Haupt Bugtracking System
- Anlegen eines Bugzilla Eintrags mit:
  - Details des Problems
  - betroffene Produkte
  - Sourcepatches für Fix
  - Exploits (wenn vorhanden)
  - Priorität und Zeitrahmen für Fix
- Zuweisung an Paketmaintainer

Sicherheitsupdates - Fix

Aufgaben des Paketmaintainers bei Updates:

- Patch reviewen
- Paket(e) aus alten Source repositories holen
- Paket(e) mit Patch versehen
- Testen ob Paket(e) baut
- Paket(e) in alte Sourcerepositories abgeben

Aufgabe des Bausystem Teams:

- Review der abgegebenen Pakete
  - Patch wird applied
  - Patch macht nichts falsches

Sicherheitsupdates – Patch & QA

- Metainformation für Online Update Struktur (Patch)
  - Betroffene Pakete und Distributionen
  - Beschreibungen (englisch und deutsch)
- Bausystem baut Struktur (RPMs + patch file) für Online Updates
- Test durch QA Team:
  - Problem existiert vorher
  - Online Update funktioniert und installiert neue Pakete
  - Abhängigkeiten sind unverändert
  - Probiem existiert jetzt nicht mehr
  - Paket wird getestet nach internen Testvorschriften

Sicherheitsupdates - Release

- Security Team stößt Release der Pakete an
- Updates werden automatisch auf Mirrorstruktur verteilt
- Business Kunden erhalten Benachrichtung
- Security Team schreibt Security Advisory
- Information der Kunden:
  - Erhalten Benachrichtigungen per Mail pro Patch
  - Benachrichtigung durch SUSE Watcher (per Popup / Icon)
  - Online Update via Cron Job
  - Security Advisories (suse-security-announce@suse.com), RSS, http://www.novell.com/linux/security/

Empfehlungen an Kunden

- Reduktion laufender Systemdienste
- minimale Anzahl Accounts
- gute Passwörter!
- keine Klartext Dienste mit Passwörtern
  - POP3, IMAP4, FTP
- Sicherheitsupdates installieren!
  - suse-security-announce@suse.com
  - KDE/GNOME Panel Icon – SUSE Watcher
  - Cron job

Fragen?