IT-Security durch das passende OS. Oracle Solaris 11.2.

Heiko Stein
Senior IT-Architekt
etomer GmbH

Agenda.

- Motivation (?)
- Compliance und Security in Solaris 11.2
  - Besondere Funktionen und deren Nutzung
- Zusammenfassung

Motivation (1).

- Technisch komplexere Attacken/Angriffszenarien
- Intelligente/kürzere und kombinierte Angriffswege
- Angriffe auf kritische Infrastrukturen
- Hacktivismus/Professionalisierung, Kriminalisierung der "Szene„

Motivation (2).

- Angriffe auf Closed-Source-Systeme
- BYOD
- 70 bis 80 Prozent aller Sicherheitsvorfälle sind Insider-Threats
- Angriffe/Vorfällen von "Innen" ~25% - 35%
  - (hohe Dunkelziffer, insbesondere bei Vorfällen durch oder wegen Fehlbedienung...)

Motivation (3).

In das OS integriert

Einbindung in den Lifecycle des OS

Umfassend

Standards

Hardening per Default

Auditierbar

Compliance und Security in Solaris 11.2 (1).

Compliance
- SCAP based compliance(1M) with Solaris & PCI-DSS Policies
- Immutable Global Zone
- Puppet

Authentication
- Trusted Path Console login
- Kerberos for unattended long running jobs

Audit
- Administrative intent audit
- Time & Size based log rotation
- Puppet audit records

Delegation
- Time & Location based RBAC
- Authenticated Access Profiles

Compliance und Security in Solaris 11.2 (2).

Data Security
- IKEv2
- ZFS Encryption Performance Verbesserungen

Installation
- SSL Install
- Unified Archives
- Installation RBAC profiles

Cryptography
- FIPS 140-2 evaluated cryptographic framework
- Camellia ciphers
- improved crypto performance SPARC & x86

Secure/verified Boot
- Verhindert Codeinjection/manipulierte Kernel /Modules
- Signed Binaries

Compliance und Security in Solaris 11.2 (3).

TPM Support

- Trusted Platform Module Support
- Trusted Platform Module driver (driver/crypto/TPM)
- TrouSerS TCG software (library/security/trousers)

ASLR (address space layout randomization)

- ASLR randomisiert die Startadresse der Segmente in virtuellen Adressspace des Prozesses
- Schutz vor Return Oriented Programming (ROP) basierten Angriffen

Secure Installation.

Automated Installer nutzt TLS (SPARC/X86)

- Server Authentication
- Client Authentication
- Verschlüsselung des Datenzugriffs
- Kontrolle des Zugriffes auf die Installationsquellen
- Verifizierung der Installationsquellen

Support für Installationsminimierung

- Neues IPS group package:
  - solaris-minimal-server

Locked down Images

- Unified Archives

Sichere IPS package repositories

- Krypthografisch validierte Paketinhalte

Secure/verified boot.

Schutz vor:

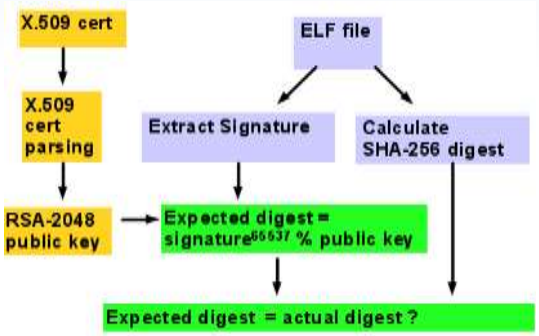
- Beschädigten/manipulierten Kernelmodulen
- Manipulierten Drittanbietermodulen
- Unauthorisierten Modulen

Bootpolicies

- boot_policy
- module_policy

Settings

- None
- Warning
- Enforce



Immutable Global Zone - Immutable Root file system.

```
# zonecfg -z global "set file-mac-profile=flexible-configuration;commit"
updating /platform/i86pc/boot_archive
updating /platform/i86pc/amd64/boot_archive

# init 6
```

```
# rm /usr/bin/ls
rm: /usr/bin/ls: override protection 555 (yes/no)? y
rm: /usr/bin/ls not removed: Read-only file system
```

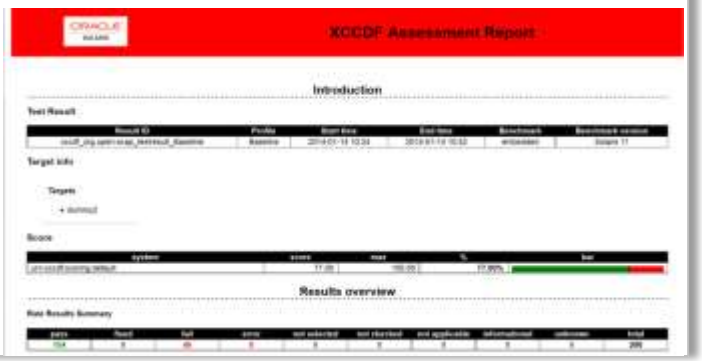
Compliance.

Konfiguration von Compliance Reporting

- CVE-Daten in IPS Metadaten
- Security Content Automation Protocol (SCAP)
- BART (… bereits in Solaris 10 …)

compliance(1M)

- Überprüfung des Systemes gegen eine definierte Policy
- Erstellung eines HTML-Bericht mit Hilfsanweisungen
- Enthaltene Policies:
  - Solaris Baseline (153)
  - Solaris Recommended (185)
  - PCI-DSS (191)
- Geplant: Authoring Tool für SCAP (XCCDF/OVAL)



Zusammenfassung.

- Umfassende ins OS integrierte Tools
- Kontinuierliche Weiterentwicklung
- In das Lifecyclemanagement des OS integriert
- Support über den kompletten Stack durch den Hersteller

Quellen.

- Oracle® Solaris 11.2 Security Compliance Guide
  - http://docs.oracle.com/cd/E36784_01/html/E39067/index.html
- Administering Network Services in Oracle Solaris
  - http://docs.oracle.com/cd/E36784_01
- Security Evaluations
  - http://www.oracle.com/technetwork/topics/security/security-evaluations-087427.html

Vielen Dank für Ihre Aufmerksamkeit.

heiko.stein@etomer.com