

Einführung in ASPE

Peter Šurda
surda@shurdix.com

WTF?

- Beobachtet / misst Verhalten von Computern
 - passiv
 - aktiv
- Reagiert darauf
- Geeignet um Sicherheitspolitik automatisiert durchzusetzen

ASPE-Module

- aspe.smtp
 - Inspiziert SMTP-Verkehr, derzeit beschränkt auf ausgehend
- aspe.vulncheck
 - Überprüft Rechner nach Sicherheitslücken, derzeit nur eine
- aspe.arpflood
 - ARP-Anfragen-Anomalien
- aspe.dhcpwatch
 - Anomalien in DHCP-Anfragen

Beobachtetes Verhalten von Computern

- verschickt Virus/Wurm über SMTP
- macht inkorrekte SMTP-Verbindungen
- Betreibt System anfällig gegen Sasser&co
- Versucht Rechner zu kontaktieren die es nicht gibt
 - Kann Netzscan sein oder Wurm, oder alte Mountpoints
- Wechselt den Rechnernamen
 - Dual-boot, Knoppix oder versucht die MAC zu faken

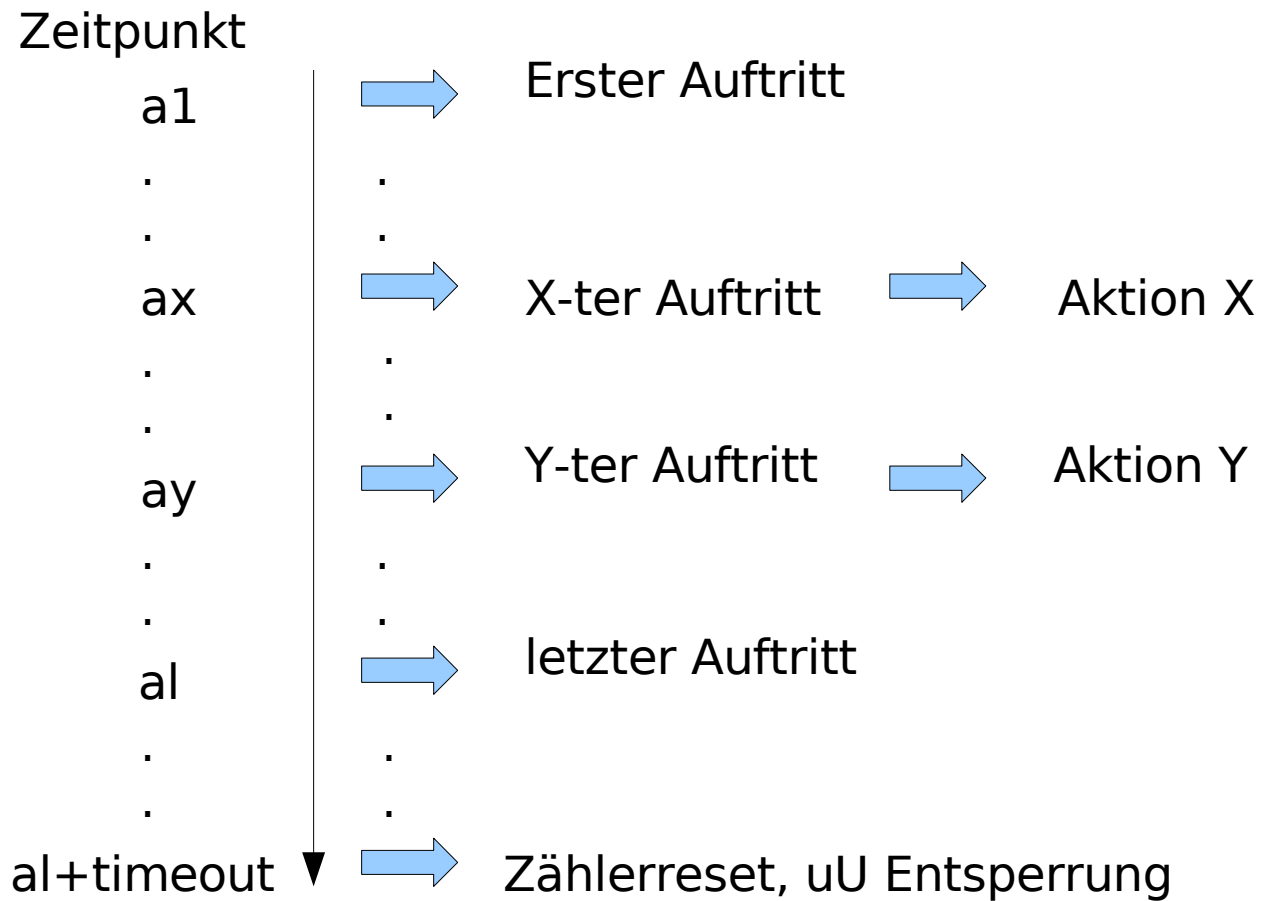
ASPE-Reaktionen

- Generische
 - Mailadmin, mail, block, unblock, winpopup
 - Externe Scripts/Programme ausführen
 - Jede Reaktionsdefinition kann eigenes Text haben
 - Nachrichten sind mit ein Paar Mustern individualisierbar (z.B. IP oder Auftrittszahl)
- Modulspezifische
 - ZB SMTP-Verkehr sperren
- Beschränkungen
 - ZB max. Verbindungsanzahl, max. Scanfrequenz

Reaktionsmessung

- Immer pro-IP gemessen
- Auftrittszähler
- Zeitpunkt des letzten Auftritts

Reaktionsablauf



Konfiguration

- /etc/sysconfig/aspe*
- Dokumentiert unter <http://docs.shurdix.org/aspe:config>
- Webinterface in Arbeit

Aktivieren

- (boot) In `/etc/sysconfig/services`
- (interaktiv) `service aspe_wasauchimmer start`
- Reaktionen lassen sich auch manuell hervorrufen, z.B. `echo "Machst Unsinn wirst gesperrt" | aspe.action.pl -M -b -s Warnung 10.1.20.51`

Schwierigkeiten

- Keine direkt zeitabhängige Reaktionen
 - Lässt sich durch Scanfrequenz simulieren
- Entsperrung als Reaktion kann unbeabsichtigte Folgen haben

Herausforderungen am Campus

- Skript für Sperren/Entsperren
- Testen

Konfiguration am Campus

- Benachrichtigung sobald ein Verstoß wenig zweifelhaft erscheint
- Nach einiger Zeit eventuell strenger formulierte Benachrichtigung
- Sperren nach einer sinnvollen Zeitperiode
- In der Testphase nur Benachrichtigung vom Admin

THNX

;-)