HET **BEWAKEN** VAN DE **SYSTEEM-HARDENING**

Het doel van systeem hardening is om zo veel mogelijk veiligheidsrisico's te elimineren. Dit wordt over het algemeen gedaan door overbodige functies en/of software van het besturingssysteem uit te zetten of van het systeem te verwijderen. Denk daarbij aan het uitschakelen of verwijderen van onnodige gebruiker-accounts en systeemservices, het aanscherpen van het wachtwoordbeleid, de toegang tot bestanden en directories, systeemrechten, kernel-parameters, netwerkinstellingen en het patchbeleid.

Hardening is nodig om de toegang tot een systeem zo moeilijk mogelijk te maken. En, als het een aanvaller dan toch lukt om toegang te krijgen, dan dient het systeem zodanig gehardend te zijn dat die aanvaller weinig kan uitrichten.

Bewaken en auditen
Als een systeem eenmaal gehardend is, betekent dat niet dat het daarmee klaar is. Deze hardening moet namelijk bewaakt worden en regulier geaudit worden. Beheerders en softwareleverancier zijn gewend om volledige toegang te hebben tot systemen met alle bijbehorende rechten. En als een systeem gehardend is, dan worden die rechten aardig ingeperkt. Bij werkzaamheden op een systeem kan het dus voorkomen dat er onderdelen van hardening uitgezet of aangepast worden omdat dan bijvoorbeeld de installatie van software beter gaat. Die aangepaste onderdelen worden dan meestal niet meer teruggezet. Beetje bij beetje kan het dus gebeuren dat de zorgvuldig geïmplementeerde hardening in de loop van de tijd zwakheden gaat vertonen.

Monitoring hardening
Gensys monitoring heeft de mogelijkheid om deze hardening te bewaken. Hoe werkt dat bij Red Hat 7? In de hardening laag van de Red Hat 7 monitoring-template bevinden zich elf objecten die elk bepaalde controles uitvoeren.

In de tabel onderstaande wordt weergegeven welke controles elk object uitvoert:

object	omschrijving	score
mounts	controleert op aanwezigheid en instellingen van opties voor gemounte filesystemen	13
permissions	controleert de permissies en ownership van systeembestanden, systeem-executables en shared libraries	22
selinux	controleert de status, huidige mode en configuratiemode van Security Enhanced Linux	7
sysctl	controleert de waarden van een subset van dynamic kernel parameters	18
trusted	Controleert trusted hosts en users en de hosts.allow en hosts.deny configuratie	4
firewall	controleert of de firewalld of iptables firewall service actief is of niet	1
sshd_config	controleert de parameters en waarden van de SSH serverconfiguratie	14
authentication	controleert de instellingen voor authenticatie	18
legacy	controleert of de legacy services en clients op het systeem geïnstalleerd zijn	14
unowned	controleert of er bestanden en directories op het systeem aanwezig zijn waar geen eigenaar of groep aan toegewezen zijn	0
remainder	voert de controles uit voor hardening die buiten de categorie vallen van de aanwezige objecten	10

Bron: CIS Security Benchmarks

Als op de hardening-laag ingezoomd wordt, dan wordt de score op 0 gezet. Op elk object worden verschillende tests uitgevoerd om de huidige status van hardening-onderdelen te controleren. De score wordt opgehoogd met 1 als een hardening-onderdeel correct is geconfigureerd. Elk object kan deze score ophogen met maximaal de waarde zoals aangegeven in de scorekolom in voorgaande tabel. Als er uitgezoomd wordt vanuit de hardening-laag dan wordt een percentage berekend dat aangeeft in welke mate het systeem voldoet aan de best practices voor systeem-hardening. Een score van 100% is het ultieme doel. Maar veelal is dat niet mogelijk omdat bepaalde hardening-onderdelen voor een specifieke serverfunctie onwenselijk kunnen zijn.

Afwijking is een Change
Het berekende percentage wordt bij de betreffende configuration item (CI) in de Active CMDB van Gensys opgeslagen. Als dat nieuwe percentage afwijkt van het eerder berekend percentage wordt een melding gegenereerd en omdat hardening is bedoeld om een gewenst niveau van beveiliging te handhaven, wordt een afwijkend percentage gezien als een 'change'. Die wijziging dient binnen het change management proces door (een) bevoegde medewerker(s) wel of niet geaccepteerd te worden, waarbij o.a. gebruik gemaakt kan worden van opgeslagen meldingen over de uitgevoerde controles op de objecten. Ook kan het verloop van het hardening-percentage worden getoond omdat historische informatie wordt bewaard.

Meer over systeem-hardening
Meer informatie over systeem-hardening kan gevonden worden op de CIS Security Benchmarks website (http://benchmarks.cisecurity.org). Op de website zijn benchmarkdocumenten te downloaden voor een scala aan desktopsoftware, mobile devices, network devices, operating systems en serversoftware. Het CIS Security Benchmarks programma biedt goed gedefinieerde, onpartijdige en op consensus gebaseerde best practices om organisaties te helpen met het auditen en verbeteren van hun beveiliging.