TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Hardening

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Hardeningbeleid voor gemeenten’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Doel

Dit document beschrijft de beleidsuitgangspunten ten aanzien van informatiebeveiliging voor een invulling van het hardening beleid door organisaties binnen de Rijksoverheid. Deze uitgangspunten over informatiebeveiliging zijn afkomstig uit de BIR en het beleid voldoet daarmee aan de BIR.

Doelgroep

Dit document is van belang voor de directie voor wat betreft de aanvulling van het informatiebeveiligingsbeleid voor hardening, en het technisch beheer en systeembeheerder voor de implementatie en uitvoering van hardening.

Reikwijdte

Dit document heeft voornamelijk betrekking op maatregelen 10.4.2.2, 10.6.1.2, 11.4 en 12.4.1 van de Baseline Informatiebeveiliging Rijksdienst (BIR). Het document gaat in op personele, organisatorische en technische informatiebeveiligingsaspecten die organisaties binnen de Rijksoverheid dienen te overwegen in relatie tot hardening.

Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Informatiebeveiligingsbeleid
- Patch management

Inhoudsopgave

1 Inleiding

Eén van de makkelijkste doelen voor een aanvaller is een niet goed actueel gehouden systeem met de laatste patches en updates, en een systeem waarbij functionaliteiten en privileges niet zijn teruggebracht tot het minimum dat noodzakelijk is voor het uitvoeren van de taak. Hardening is het proces waarbij overbodige functies in besturingssystemen en andere software uitgeschakeld worden en/of van het systeem verwijderd worden. Daarnaast hoort bij hardening dat zodanige waarden worden toegekend aan beveiligingsinstellingen dat hiermee de mogelijkheden om een systeem te compromitteren worden verlaagd en een maximale veiligheid ontstaat. Het kan bijvoorbeeld gaan om het verwijderen van niet gebruikte of onnodige gebruikersaccounts, en tevens het wijzigen van standaard wachtwoorden die op sommige systemen aanwezig kunnen zijn.

Hardening betreft servers, actieve netwerkcomponenten, zoals Firewalls en switches, desktops, laptops, mobiele devices. Kortom, de gehele electronische informatievoorziening. Het resultaat is een *gehard* systeem.

1.1 Aanwijzing voor gebruik

Dit document is geschreven om informatiebeveiligingsmaatregelen met betrekking tot hardening te duiden en te verscherpen. De BIR geeft enkele maatregelen die op hardening ingaan en die in dit document nader worden toegelicht. Deze handleiding is geen volledige procesbeschrijving en bevat geen productbeschrijvingen. Het bevat informatie om goede keuzes te kunnen maken en bewustwording te creëren met betrekking tot hardening van systemen.

1.2 Leeswijzer

In dit document volgt eerst een algemene beschrijving van hardening en het hardening proces. Afsluitend bevat dit document een aanvulling op het beveiligingsbeleid voor hardening.

2 Hardening

2.1 Inleiding

Hardening is het proces waarbij overbodige functies uitgeschakeld worden en/of van het systeem verwijderd worden. Hardening van de actieve infrastructuur, servers en netwerkcomponenten, is een belangrijke stap om persoonlijke gegevens en informatie te beschermen. Er zijn diverse methoden die betrekking hebben op hardening van systemen. In basis gaan alle methoden volgens een vast patroon te werk zodat niets vergeten wordt. De methoden zijn specifiek bedoeld voor hardening van Windows systemen, hardening van Linux systemen, hardening van webservers etc.

Een goede computerbeveiliging vindt de juiste balans tussen het hardenen van de systemen tegen mogelijke bedreigingen versus functionaliteit. Als een bepaalde software applicatie of service niet nodig is, moet deze worden uitgeschakeld en verwijderd. Extra software die aanwezig is, vereist meer werk van de systeembeheerders om een systeem te beheren en vergroot de kans dat een aanval succesvol kan worden uitgevoerd. Onnodige software toevoegen kan ervoor zorgen dat een computer een lanceerplatform wordt voor de verspreiding van een virus en tevens voor een hacker een toegangspoort wordt om andere systemen binnen het netwerk te kunnen aanvallen.

Hardening heeft de volgende doelstellingen:

- de reductie van de mogelijkheden om zwakheden te benutten op systemen;
- het tegenwerken van een aanvaller die binnengedrongen is door de mogelijke programma's en tooling op systemen te minimaliseren;
- het tegenwerken van een aanvaller die binnengedrongen is door het minimaliseren van ter beschikking staande systeemrechten;
- het verhogen van de mogelijkheden van detectie bij een gelukte aanval;
- het verminderen van systeem complexiteit en daarmee een verbeterde beheersing van het systeem en lagere beheerkosten.

2.2 Verdediging in lagen ("Defence in Depth")

Hardening van een computer omvat verschillende stappen die samen verschillende beschermingslagen vormen. Deze benadering wordt vaak genoemd: 'verdediging in lagen'. Maatregelen voor hardening staan nooit op zichzelf. Er dienen ook andere maatregelen te worden uitgevoerd, zoals patchmanagement, antivirusoplossingen, logging, firewalls, en IDS en IPS[1], die allen bijdragen aan een verdediging in lagen-strategie.

[1] Intrusion detection system en intrusion prevention systemen.

Het regelmatig toepassen beveiligingspatches van leveranciers is de eerste stap om computersystemen te hardenen. Een andere laag van bescherming voor computers is het installeren en regelmatig gebruiken van software voor antivirus- en antispyware. Het plannen van dagelijkse automatische definitie-updates en automatische scans op computers zijn hierbij essentiële stappen.

Ook adviseren veel beveiligingsexperts het installeren van een softwarematige firewall op de computer. Extra hardeningacties omvatten het afsluiten van serverpoorten, het uitschakelen van delen van besturingssystemen en andere programma's waaronder file-sharing en e-mailprogramma's.

2.3 Processtappen bij hardening

Het is verstandig om een bepaalde volgorde aan te houden bij het hardenen van systemen om de kans te verkleinen dat iets vergeten wordt. Er zijn soms specifiek voor bepaalde besturingssystemen of software hardening aanwijzingen beschikbaar. Het hardeningsproces dient de volgende stappen te bevatten, waaronder het:

- verwijderen of deactiveren van software componenten die niet direct noodzakelijk zijn;
- verwijderen of deactiveren van onnodige gebruikers accounts;
- niet gebruiken van het administrator account of administrator account rechten voor server processen;
- gebruik van alleen sterke wachtwoorden van minimaal 8 tekens van gemengde samenstelling;
- veranderen van standaard wachtwoorden in systemen;
- gebruik van de firewall;
- installeren van antivirus software;
- deactiveren van alle onnodige services en poorten;
- optimaliseren van rechten op het bestandssysteem;
- inzetten van mandatory access control[2];
- gebruiken van uitsluitend versleutelde dataverbindingen;
- zo veel als mogelijk gebruiken van foutloze en (automatisch) gepatchte software.

Een gehardened besturingssysteem heeft de volgende kenmerken:

1. Alles wat nodig is voor het systeem is geactiveerd, alle onnodige diensten, poorten en componenten zijn gewist of uitgeschakeld;
2. Alle niet benodigde gebruikersaccounts zijn gewist;
3. Alle niet benodigde poorten zijn gesloten;
4. Rechten zijn zoveel als mogelijk beperkt.

[2] Mandatory Access Control vrij vertaald "verplichte toegangscontrole" (MAC) verwijst naar een soort van toegangscontrole waarbij het besturingssysteem de toegangs mogelijkheden beperkt tot bijvoorbeeld bestanden of objecten door gebruikers of systeemprocessen, dit kan centraal worden geregeld.

2.4 Hardening testen en monitoren IT systemen

Monitoring door middel van Security Information and Event Management (SIEM) is ook een middel dat kan bijdragen aan een goed gebruik van software en hardware. SIEM-technologie biedt een real-time analyse van beveiligingswaarschuwingen gegenereerd door netwerk-hardware en applicaties. SIEM-oplossingen kunnen bestaan uit software, apparaten of managed services, en worden ook gebruikt voor het loggen van beveiligingsincidenten en het genereren van rapportages op naleving van doeleinden.

Hardening kan deels getest worden door middel van de genoemde vulnerability scanners voor patchmanagement, daarnaast zijn er ook producten die scannen op zwakheden.

2.5 Links

NCSC webrichtlijnen

https://www.ncsc.nl/binaries/nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties/1/ICT%2Bbeveiligingsrichtlijnen%2Bvoor%2Bwebapplicaties%2B%2B%2Bdeel%2B1%2B%2Bleesversie%2B.pdf

Enkele Microsoft TechNet links en de laatste link naar Microsoft tooling

http://technet.microsoft.com/en-us/library/dd277465.aspx

http://technet.microsoft.com/en-us/library/cc995076.aspx

http://technet.microsoft.com/en-us/library/cc526440.aspx

http://www.microsoft.com/en-us/download/details.aspx?id=7558

Apache hardening handleidingen

http://xianshield.org/guides/apache2.0guide.html

http://people.apache.org/~sctemme/ApconUS2008/hardening.pdf

Bijlage 1: Hardening beleid <organisatie>

Het hardening beleid van <organisatie> geeft richting aan de wijze waarop de organisatie maatregelen wenst te treffen voor hardening. <Organisatie> onderschrijft het belang van een adequaat hardening beleid omdat het niet uitvoeren van hardening ernstige schade kan toebrengen aan systemen en de informatievoorziening in termen van beschikbaarheid, exclusiviteit (vertrouwelijkheid) en integriteit. Bovendien kan het niet uitvoeren van hardening schade toebrengen aan het belang van de burger en het vertrouwen in de organisatie. Hardening dient gestructureerd te worden aangepakt en er moeten procedures worden vastgesteld om hardening doeltreffend en ordelijk te laten plaatsvinden. Dit beleid is van toepassing op alle systemen die in gebruik zijn is bij <organisatie>.

De volgende uitgangspunten zijn vastgesteld voor de organisatie en deze zijn ontleend aan het informatiebeveiligingsbeleid, de Code voor Informatiebeveiliging (NEN/ISO 27002:2007) en de BIR:

1. Om te voorkomen dat schadelijke software kan worden uitgevoerd door middel van een browser dient de mogelijkheid van een gebruiker om mobiele code uit te voeren te worden beperkt. Daarnaast dienen de instellingen die dit mogelijk maken te worden geblokkeerd door middel van een systeem policy. Gebruikersrechten worden beperkt tot het minimaal noodzakelijke;
2. Gegevensuitwisseling tussen vertrouwde en niet-vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware;
3. Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst, dienen te worden afgesloten door systeembeheerders;
4. Op alle apparatuur waar dit mogelijk is, worden beschikbare firewalls, antivirusscanners en andere beschermende maatregelen geactiveerd;
5. Op alle apparatuur wordt (waar mogelijk) systeem logging geactiveerd om detectie mogelijk te maken van malware en ongebruikelijke systeem activiteiten;
6. Werkstations worden zo ingericht dat routeren van verkeer tussen verschillende zones of netwerken niet mogelijk is;
7. De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze zich bevinden. Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden;
8. Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen);
9. Alleen geautoriseerd personeel kan functies en software installeren of activeren;
10. Voor toegang tot systemen door middel van wachtwoorden wordt wachtwoordbeleid nageleefd;
11. Alle apparatuur moet regelmatig worden getest op bekende zwakheden.

Aldus vastgesteld door de directie van *[organisatie]* op *[datum],*

[Naam. Functie] [Naam. Functie]

_____ _____