TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Anti-malware beleid

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 ‘Anti-malware beleid’ 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 biedt een handreiking voor beleidsuitgangspunten voor de invulling van anti-malware beleid voor organisaties binnen de Rijksoverheid. Deze uitgangspunten zijn afkomstig uit de BIR en het beleid voldoet daarmee aan de BIR.

Doelgroep

Dit document is van belang voor het verantwoordelijke lijnmanagement van de organisatie, systeembeheer en gebruikers. Het management is verantwoordelijk voor de invulling van het beleid. Systeembeheer en gebruikers zijn verantwoordelijk voor de uitvoering van het beleid.

Reikwijdte

Dit document heeft voornamelijk betrekking op maatregelen 7.1.3, 10.4.1, 10.6.1, 10.8.1, 10.10.2, 11.7.1, 11.7.2, 12.6.1 en 13 van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Mobiele apparaten

Inhoudsopgave

1 Anti-malware beleid

Dit document biedt een handreiking voor beleidsuitgangspunten voor de invulling van anti-malware beleid voor organisaties binnen de Rijksoverheid. Deze beleidsuitgangspunten zijn afkomstig uit de BIR en het beleid voldoet daarmee aan de BIR. Een voorbeeld voor invulling van het anti-malware beleid voor een overheidsorganisatie op basis van de beleidsuitgangspunten is beschreven in de bijlage 'Anti-malware beleid'.

In dit document wordt de voorkeur gegeven voor de term *malware* in tegenstelling tot *virus*. Een virus is een variant van malware.

1.1 Wat is malware?

Malware is een samenvoeging van het Engelse *malicious* en *software* (kwaadwillende software) en een verzamelnaam voor kwaadaardige en/of schadelijke software. Malware behoort tot de grootste bedreigingen van ICT-infrastructuur en de daarbinnen aanwezige bedrijfsinformatie door gebruik te maken van zwakheden in software (soms ook in hardware) en onachtzaamheid van gebruikers. De gevolgen van een malware-infectie kunnen zeer schadelijk en riskant zijn, en leiden tot uitval van systemen, vertraging bij het gebruik van systemen, overname van controle over systemen, het niet beschikbaar zijn van informatie of zelfs het verlies van informatie. Er zijn verschillende malware-varianten. De volgende varianten behoren tot de meest voorkomende malware: virus, worm, spyware, adware, trojan, tracking cookie, dropper, dialer, rootkit, backdoor, rogueware, ransomware.

1.2 Ontwikkelingen in malware

In het begin van de desktop automatisering bestond malware vooral uit bootsector virussen, gewone virussen en eenvoudige wormen.[1] Het doel van deze virussen was schade aan te richten op hun gastheer en zichzelf te vermenigvuldigen. In deze tijd werd er nog veel gewerkt met floppy's en dus was een bootsector virus[2] de manier om ervoor te zorgen dat de besmetting overal terecht kwam. In deze tijd was er al een fenomeen in opkomst om geld te verdienen met malware en dat was de zogenaamde 'Dialer'. Deze vorm van malware gaf de computer instructie om via het modem verbinding te maken met betaalde telefoonnummers waardoor aanzienlijke kosten ontstonden.

De toepassing van malware wordt steeds professioneler en beter georganiseerd. Partijen die malware inzetten hebben vaak het belang om informatie te stelen. Informatie is (direct of indirect) immers geld waard. Om dit doel te bereiken, zullen deze partijen ervoor zorgen dat hun malware zo lang mogelijk niet ontdekt blijft.

Randsomware is een andere bekende vorm van malware. Deze op een doelsysteem geplaatste kwaadwillende software, versleutelt data of blokkeert het gebruik van het systeem. Voor het ontsleutelen van data of het deblokkeren van systemen wordt 'losgeld' geëist.

[1] Door de relatieve eenvoud van de gebruikte code konden oude virussen en wormen relatief eenvoudig ontdekt worden.
[2] Een virus die zich nestelt in de eerste sector van een disk.

1.3 Malware aanval

De laatste jaren wordt tijdens een gerichte malware-aanval tegelijkertijd gebruik gemaakt van verschillende soorten malware om zo de kans op een besmetting van een systeem te vergroten. Deze aanvallen doen zich meestal voor in een zogenaamde drive-by aanval, waarbij een kleine besmetting in bijvoorbeeld een advertentie, bijlage of weblink zorgt voor het ophalen van verschillende malware van speciaal daarvoor ingerichte servers en het plaatsen ervan op systemen. Deze geplaatste code kan op twee manieren worden geactiveerd: automatisch of door een muisklik van de gebruiker. De drive-by aanval is op dit moment de meest gebruikte manier om systemen te besmetten en informatie te stelen.[3]

1.4 Anti-malware maatregelen

Maatregelen tegen malware richten zich op beleid, bewustwording, processen en ICT. Individuele maatregelen richten zich op een (facet van een) beveiligingslaag en werken het beste in samenhang. Voor de organisatie is beleid, en het naleven daarvan, van wezenlijk belang evenals het oefenen van scenario's waarbij de bedrijfsvoering verstoord wordt. Voor gebruikers is bewustwording van het risico van malware essentieel om zo de benodigde aanpassing van het gedrag te bereiken. Voor systeembeheer is patch management de belangrijkste maatregel en het technisch laten functioneren van anti-malware software op de verschillende ICT-componenten.

Het Forum Standaardisatie geeft een aantal maatregelen tegen malware.[4] De maatregelen richten zich onder meer op mail. Over het algemeen wordt er bij anti-malware gericht op het risico van binnenkomende mail voor gebruikers met bijvoorbeeld malware in de bijlage of achter links. Er zijn echter ook maatregelen die betrekking hebben op uitgaande mail. Het is bijvoorbeeld raadzaam om een Sender Policy Framework (SPF) in te richten dat het verzenden van spam vanuit de overheidsorganisatie beperkt. Ook een Domain Keys Identified Mail (DKIM) vermindert het verzenden van spam door authenticatie van mail vanuit organisaties te versterken. De reputatielijsten die DKIM oplevert, kunnen gebruikt worden tegen spam.

1.5 Verantwoordelijkheden en taken

De verantwoordelijkheden en taken ten aanzien van anti-malware beleid zijn als volgt in te vullen:

Bestuurder

De bestuurder dient actief het beleid uit te dragen en de juiste uitvoering van het beleid te controleren. Een bestuurder heeft daarnaast een voorbeeldfunctie en is tegelijkertijd ook gebruiker van ICT-voorzieningen.

[3] Zie: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape /at_download/fullReport
4 https://lijsten.forumstandaardisatie.nl/

Management

Het management is verantwoordelijk voor het aansturen van het personeel in de meest brede zin en moet ervoor zorgen dan alle gebruikers zich bewust zijn van de risico's van internet en computergebruik. Het management dient een actieve rol te hebben in het aansturen van bijvoorbeeld systeembeheer en het zorg dragen voor de opvolging van rapportages.

CISO

De CISO ondersteunt gevraagd en ongevraagd bestuurders en management bij het inrichten en uitvoeren van het beleid, beoordeelt de rapportages en bereidt rapportages voor en doet aan trendanalyses. De CISO ondersteunt het systeembeheer bij het inrichten van patch management en anti-malware maatregelen. De CISO heeft een actieve rol in het Incident Response en Management proces.

Systeembeheer

Systeembeheer is verantwoordelijk voor het proces rondom de malware-bestrijding. Dit geldt zowel voor preventieve als repressieve maatregelen, waaronder het:

- uitvoering van het patch management. Alleen als een patch of update een verstoring van de ICT-dienstverlening veroorzaakt, mag een patch of update worden uitgesteld. In dat geval moeten andere manieren worden gezocht om de zwakke plek in het systeem af te schermen, zodat het systeem minder kwetsbaar is bij onjuist gebruik of pogingen tot misbruik;
- elimineren van de zwakheid en het beschermen van systemen tegen onjuist gebruik of misbruik;
- zorg dragen voor een up-to-date anti-malware systeem op alle devices van de organisatie inclusief anti-spam maatregelen binnen de mailomgeving en controleert daarvan dagelijks de werking en de gedetecteerde malware of andere verdachte software;
- zorg dragen voor een up-to-date firewall en controleert daarvan dagelijks de logging;
- monitoring van zowel inkomend netwerkverkeer als uitgaand netwerkverkeer;
- Mailrelaying[5] voorkomen door het dichtzetten van poort 25 voor alle andere mailservers dan de eigen mailserver;
- zorg dragen voor hardening van systemen;[6]
- voorkomen dat (bv. MS Office) macro's en scripts ongecontroleerd uitgevoerd kunnen worden;
- technisch afdwingen van gedragsregels;
- maandelijks rapporteren aan de CISO over de aantallen gedetecteerde aanvallen, over de werkplekken die besmet zijn, de ondernomen acties om besmettingen te mitigeren.

[5] Mailrelaying is mail versturen via een andere mailserver dan de standaard mailserver binnen een netwerk of domein. Spammers maken gebruik van mailrelaying om spam mail te versturen. Zombie pc's proberen ook vaak van relaying gebruik te maken.
[6] Hardening is het zorgdragen dat alleen die functies en software op een systeem draaien die nodig zijn, daarmee worden aanvalsmogelijkheden beperkt.

Gebruikers

Gebruikers dienen zich de gedragsregels voor computer gebruik eigen te maken. Een malware besmetting is altijd een incident dat ook gemeld moet worden in de lijn en aan de CISO.

In deze gedragsregels moet minimaal worden opgenomen:

- hoe om te gaan met mobiele media (en dat deze regels waar mogelijk afgedwongen worden door technische maatregelen);
- het gebruik van USB-sticks tegen gaan of alleen gebruik te maken van speciale USB-sticks en/of speciale stations (bijvoorbeeld encrypted USB-sticks);
- het niet klikken op links in e-mails die niet verwacht worden;
- het niet openen van bijlagen die er verdacht uitzien, die niet worden verwacht door de gebruiker of van onbekenden afkomstig zijn.
- het verplicht melden van verdacht gedrag van de werkplek of de software waarmee wordt gewerkt.

Bijlage: Anti-Malware beleid <organisatie>

Het anti-malware beleid van <organisatie> geeft richting aan de wijze waarop de organisatie maatregelen wenst te treffen voor een adequate detectie, preventie en herstel van verstoringen als gevolg van malware. De organisatie onderschrijft het belang van een adequaat anti-malware beleid omdat malware ernstige schade kan toebrengen aan systemen. Ook kan het de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening van de organisatie verstoren. Bovendien kan malware schade toebrengen aan het belang van de burger en het vertrouwen in de organisatie. Malware besmettingen zijn incidenten die gestructureerd moeten worden aangepakt en er moeten procedures worden vastgesteld om de reactie op deze besmettingen doeltreffend en ordelijk te laten plaatsvinden. Dit beleid is van toepassing op iedereen die werkzaam is bij de organisatie.

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

1. Het is verboden om ongeautoriseerde software te draaien op computersystemen van de organisatie. Computersystemen zijn: smartphones, tablets, desktops, laptops en servers.
2. Alle computersystemen zijn altijd voorzien van de laatste firmware, software updates en patches, tenzij door een risicoafweging is vastgesteld en geaccordeerd dat een bepaalde software-update de dienstverlening van de organisatie kan verstoren (wijzigingsbeheer). In dat geval moeten er andere maatregelen worden onderzocht en genomen.
3. Op alle systemen van de organisatie is anti-malware software aanwezig die geautomatiseerd controleert op de aanwezigheid van virussen, trojans en andere malware waarbij onderscheid gemaakt wordt tussen werkplekken en servers. De organisatie maakt gebruik van verschillende anti-malware oplossingen op verschillende schakels binnen de infrastructuur.[7]
4. Alle binnenkomende en uitgaande e-mails worden gecontroleerd op malware.
5. Het Domain Keys Identified Mail (DKIM) mechanisme wordt ingericht ten behoeve van de uitgaande mail.
6. De anti-malware software wordt iedere dag automatisch voorzien van nieuwe updates van virusdefinities en dit moet centraal bewaakt worden. Uitzonderingen hierop moeten actief worden gemonitord en gerapporteerd aan het management en aan de CISO.
7. Malware besmettingen of vermoedens daaromtrent dienen onverwijld gemeld te worden volgens de incidenten procedure.
8. Als 'mobiele code' vereist is voor het uitvoeren van de geautomatiseerde werkprocessen dan mag dat alleen tegen minimale rechten. De gebruiker mag geen extra rechten kunnen geven aan mobiele code, tenzij het management dat geaccordeerd heeft.

[7] Dit wordt gedaan om te voorkomen dat een product of oplossing nooit alleen de zwakste schakel wordt bij een uitbraak.

9. Alle malware besmettingen zijn incidenten van de zwaarste categorie.
10. Alle gebruikers zijn verplicht deel te nemen aan bewustwordingstrainingen.

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

[Naam. Functie] [Naam. Functie]

_____ _____