Colofon:

Versie : 1.0
Datum : 07-05-2024
Redactie : CIO-Rijk/CISO-Rijk
Contact : CISORijk@minbzk.nl

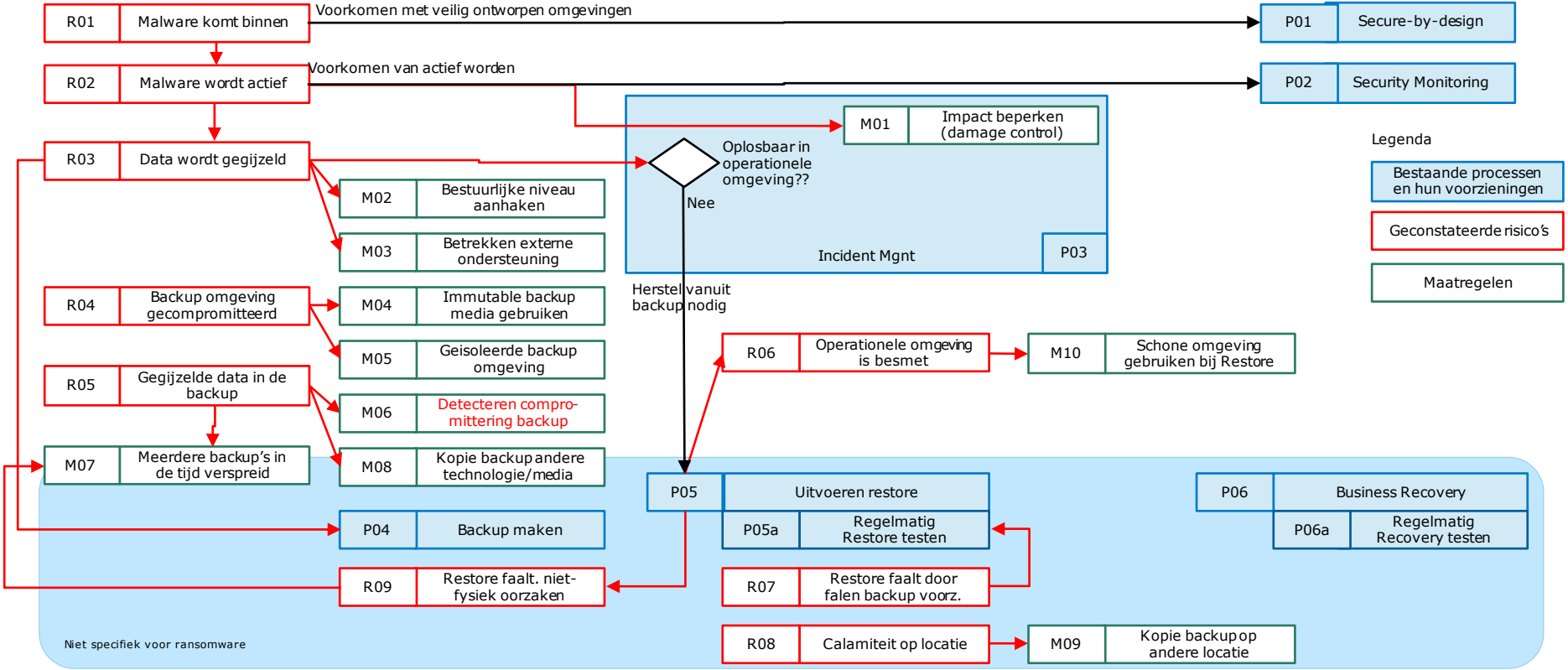
Dit document is bedoeld om organisaties te helpen om een betere bescherming tegen ransomware te geven. Het document is tot stand gekomen in samenwerking met een rijksbrede werkgroep als onderdeel van de I-strategie, thema 2 'Digitale weerbaarheid'.

Ransomware en Backups

> Risico's en Maatregelen

> Doelgroep van dit document is: IT Architecten, IT Management & Directie

Risicoanalyse



Toelichting

	Geconstateerde risico's		Te treffen maatregelen / te nemen actie		Bestaande processen
R01	Assume breach – deel 1: malware en/of ransomware is naar binnengekomen bijvoorbeeld via phishing of een malafide update	M01	Het direct treffen van maatregelen om verdere uitbraak te voorkomen zoals afsluiten van het compartiment, zie ook het kennisdocument 'Detectie en schadebeperking'. (Correctief)	P01	Het conform het secure-by-design realiseren van voldoende beveiligde operationele voorzieningen en deze veilig houden (waaronder vulnerability en patch management). Inclusief detectie van aanwezigheid van malware in data. (Preventief) (BIO 14.2, BIO 12.2, BIO 12.6)
R02	Assume breach – deel 2: de ransomware wordt actief bijvoorbeeld via rechtenescalatie	M02	Allereerst via de reguliere processen de crisisorganisatie en de bestuurlijke lijn zodat die indien nodig kunnen opschalen. (Correctief)	P02	Het monitoren van het hele ICT landschap op het actief worden/zijn van ransomware (Detectief) (BIO 12.4.1)
R03	Het gijzelen van de data gebeurt niet altijd direct na de besmetting met ransomware. Het moment van daadwerkelijke gijzeling van data wordt soms bewust vertraagd om detectie uit te stellen, de verspreiding groter te maken en herstel moeilijker te maken.	M03	Overweeg bij datagijzeling om externe organisaties zoals het High-Tech-Crime bij de politie, CSIRT's en het NCSC te betrekken: die hebben specifieke kennis en ervaring waarvan gebruik gemaakt kan worden.	P03	Het afhandelen van (beveiligings)incidenten (Correctief) (BIO 16.1)
R04	De backupomgeving zelf is gecompromitteerd door de aanwezigheid van ransomware of doordat backups zijn weggegooid. Hierdoor heb je geen toegang tot de backups.	M04	Gebruik van immutable media: daarmee wordt voorkomen dat bestaande backups worden aangetast of verwijderd. (Preventief)	P04	De specifieke processen om op 1 punt in tijd een intern-consistente backup te maken van een of meer systemen/data verzamelingen. (voorbereidend voor Correctief) (BIO 12.3)
R05	Besmette data in de backups opgenomen. Hierdoor zijn bepaalde backups gecompromitteerd en is een restore complexer.	M05	De backupvoorziening is geïsoleerd van de operationele omgevingen (bijv. o.a. middels een datadiode) (Preventief)	P05	De specifieke processen om 1 backup te restoren naar een operationele omgeving inclusief alle benodigde controles. (Correctief) (BIO 12.3)
R06	De operationele omgeving is (nog steeds) besmet en daardoor is het uitvoeren van een restore weinig zinvol.	M06	Werk IOC's uit om te detecteren dat ransomware actief is en om te beoordelen of de backup besmet is. Bijvoorbeeld: als het aantal bestanden op de incrementele backup plotseling sterk toeneemt, is dit een aanwijzing van een bestemming én van een besmette backup. Idem: ongebruikelijke (pogingen tot) toegang tot de backupvoorziening. (Detectief)	P06	De processen binnen Business Continuity Management die ervoor zorgen dat de systemen en processen weer in een onderling consistente toestand komen. Specifieke aandacht is nodig bij systemen die deel uit maken van een keten: "verloren geraakte ontvangen berichten" en "dubbel verzonden uitgaande berichten (Correctief) (BIO 17.1)
R07	Een restore faalt door technisch falen van de backupvoorziening, bijvoorbeeld verstoringen in gebruikte hardware of beschadiging van de fysieke dragers van de gebackupte gegevens	M07	Bewaar meerdere backups gemaakt op verschillende punten in tijd. Hierdoor wordt je minder kwetsbaar voor besmetting en andere compromittering. (Preventief)		
R08	Een calamiteit op de locatie van het operationele systeem vernietigd tegelijkertijd ook de backup van de gegevens	M08	Maak een backup te maken op verschillende media en verschillende technieken. Dit biedt bescherming tegen het falen van een individuele backupvoorziening. (Preventief)		
R09	Een restore faalt door andere oorzaken, waaronder bedieningsfouten en veranderingen in de operationele omgeving (bijv. niet backwards compatible software wijzigingen)	M09	Bewaar een backup op een fysiek andere locatie is de data. Dit biedt bescherming tegen volledige vernietiging van een locatie (Preventief)		
		M10	Schoon de operationele omgeving van de ransomware. Afhankelijk van de plaats van de besmetting (applicatie, operating systeem, data) verschillen de wijze waarop dit gebeurt zoals het nieuw aanmaken (VM) vs. schonen en isoleren (ketensystemen). Indien nodig eerst de backupomgeving schonen		