ManageEngine

A quick guide to the Cyberbeveiligingswet (Cbw)

The Cyberbeveiligingswet (Cbw) is the Dutch transposition of the EU NIS2 directive, issued by the Ministry of Justice and Security (NCTV) and the Ministry of the Interior (BZK). It raises cybersecurity and resilience obligations for essential and important entities and replaces the Wet beveiliging netwerk- en informatiesystemen (Wbni).

Sl.no	Requirement area	Article	Key controls to implement
1	Risk management & governance	Zorgplicht	• Conduct risk assessment • Define security measures • Assign board responsibility • Maintain access policies
2	Identity & access control	Zorgplicht	• Enforce multi-factor authentication (MFA) • Apply least privilege • Govern access by role • Automate joiner-mover-leaver (JML) processes
3	Asset & identity visibility	Zorgplicht	• Maintain asset inventory • Track identities and rights • Discover monitored systems • Report on access
4	Threat detection & monitoring	Meldplicht	• Correlate security events • Detect behavioral anomalies • Monitor for compromise • Watch leaked credentials
5	Incident response & mitigation	Meldplicht	• Automate containment workflows • Track incident cases • Reconstruct incident timelines • Mitigate service impact
6	Incident reporting	Meldplicht	• File early warning within 24 hours • Follow up within 72 hours • Submit final report within 1 month • Record severity and impact
7	Audit, logging & oversight	Toezicht	• Keep time-stamped audit trails • Retain logs • Generate compliance reports • Brief the governing body
8	Registration	Registratieplicht	• Keep time-stamped audit trails • Retain logs • Generate compliance reports • Brief the governing body

Source: www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

The Cyberbeveiligingswet and ManageEngine

ManageEngine offers solutions that help organizations assess cyber risk, control access, detect incidents, and demonstrate compliance under the Cbw. AD360, ManageEngine's identity and access management (IAM) solution, governs identities and access, while Log360, its security information and event management (SIEM) solution, delivers threat detection, incident response, and audit-ready logging. Together they help you implement the technical controls required under the Cbw.

How can ManageEngine help you implement the Cyberbeveiligingswet?

Multi-factor authentication

Enforce risk-based MFA and conditional access across Active Directory (AD), Entra ID, VPN, and applications so only authorized users gain entry.

Helps with Zorgplicht (2)–(3).

Role-based access governance

Restrict and certify access by role, OU, and attribute, applying the organizational measures the duty of care requires.

Helps with Zorgplicht (1)–(2).

Identity lifecycle automation

Automate provisioning and deprovisioning so access rights track authorization and standing privilege does not accumulate.

Helps with Zorgplicht (4).

Risk posture management

Scan AD and database configurations for misconfigurations and exposure points to inform the risk assessment.

Helps with Zorgplicht (1).

Threat detection & UEBA

Correlate events against MITRE-mapped rules and flag behavioral anomalies to surface significant incidents in time to report them.

Helps with Meldplicht (1).

Incident response automation

Orchestrate containment with SOAR playbooks and track cases through closure to mitigate the impact of incidents.

Helps with Meldplicht (4).

Incident timelines & reporting

Consolidate telemetry and reconstruct incident timelines to assemble the detail required for 24-hour, 72-hour, and final reports.

Helps with Meldplicht (2)–(3).

Audit trails & log retention

Record time-stamped events in a searchable archive with retention, maintaining records sufficient for verification and forensics.

Helps with Toezicht (2).

Compliance reportin

Generate audit-ready reports and dashboards that demonstrate the duty of care and reporting obligation to supervisors.

Helps with Toezicht (1).

For more information, contact sales@manageengine.com