

CyberFundamentals Basic afvinken: de checklist voor een kantoor op Canvos

Het CyberFundamentals-kader van het Centrum voor Cybersecurity België is de Belgische maatstaf voor NIS2 en voor elke organisatie die wil aantonen dat de basis in orde is. Deze checklist loopt door de maatregelen van het niveau Basic en toont per maatregel wat Canvos standaard regelt, wat u zelf instelt en wat buiten de werkplek valt. Met een afdrukbaar pdf.

Ingebouwd = staat standaard aan of één instelling · Deels = vraagt uw keuze of aanvulling · Uw beleid = buiten de werkplek

Identificeren: weten wat u hebt

	Status	Datum	Verantwoordelijke
☐ Inventaris van gebruikers en toegangen De gebruikerslijst in Organisatiebeheer toont elke account met rol, status, opslag en mailbox. Exporteer als CSV voor uw inventaris.	ingebouwd		
☐ Inventaris van toestellen Actieve sessies tonen per gebruiker toestel en browser. Laptops en telefoons zelf houdt u bij in uw eigen register.	deels		
☐ Inventaris van software en clouddiensten Canvos vervangt mail, bestanden, kantoorpakket, chat, vergaderen en wachtwoordkuis: één leverancier op de lijst in plaats van zes. Andere software blijft u zelf inventariseren.	deels		
☐ Beleid en wettelijke vereisten Een informatiebeveiligingsbeleid, GDPR-verwerkersregister en NIS2-registratie bij het CCB. Zie de checklist voor het verwerkersregister.	uw beleid		
☐ Leveranciersrisico Canvos draait in Europa met een Belgische leverancier, zonder Amerikaanse moedermaatschappij; de verwerkersovereenkomst en de locatie van de data staan vast.	ingebouwd		

Beschermen: toegang, data, back-up, bewustzijn

	Status	Datum	Verantwoordelijke
☐ Identiteiten en sterke authenticatie (MFA) Tweestapsverificatie met authenticator-app of hardware sleutel per gebruiker; één login voor alle modules.	ingebouwd		
☐ Minste privilege en rollen Rollen & Apps bepalen wie welke module ziet; bedrijfsmappen geven rechten per groep.	ingebouwd		
☐ Toegang op afstand en mobiel Mobiel beleid: schermbeveiliging, biometrische ontgrendeling, automatisch vergrendelen. Sessies zijn op afstand te beëindigen.	ingebouwd		
☐ Gegevens beschermd in rust en onderweg TLS overall, versleutelde back-ups (AES-256), dataclassificatie met labels, DLP op rijksregisternummers en IBAN's, deelbeleid met wachtwoord en vervaldatum.	ingebouwd		
☐ Back-ups gemaakt, bewaard en getest Dagelijkse versleutelde back-ups met bewaartermijnen zijn één instelling. Het jaarlijkse hersteltest plan en documenteert u zelf.	deels		
☐ Veilige basisconfiguratie en patching Servers, updates en beveiligingspatches beheert Canvos; uitvoerbare bestanden en bijlagen zijn standaard geblokkeerd.	ingebouwd		

☐	Verwijderen van toegang bij vertrek Eén account uitschakelen sluit mail, bestanden, agenda, chat en kluis tegelijk af; sessies vervallen.	ingebouwd
☐	Bewustmaking en opleiding Een jaarlijkse sessie over phishing en wachtwoorden blijft nodig. De gidsen op deze site kunt u als lesmateriaal gebruiken.	uw beleid
☐	Logboeken bijgehouden Loginlogboek en governance-gebeurtenissen, gehasht en dagelijks verankerd, bewaard volgens het retentiebeleid.	ingebouwd

Detecteren: zien wat er gebeurt

	Status	Datum	Verantwoordelijke
☐	Gebeurtenissen verzameld en gecorreleerd Elke beleidshandeling in de bewijsketen; export als CEF naar een SIEM, of CSV en JSON.	ingebouwd	
☐	Verdachte aanmeldingen Nieuw land of nieuw IP wordt gemarkeerd, herhaalde mislukte pogingen blokkeren tijdelijk, goedkeuring kan vereist zijn.	ingebouwd	
☐	Kwaadaardige code Uitvoerbare bestanden en bijlagen zijn geblokkeerd en mail wordt gefilterd op spam en malware. Eindpuntbeveiliging op laptops blijft uw keuze.	deels	
☐	Alerts naar de juiste mensen Realtime alerts en een maandelijks compliance-rapport naar de adressen die u instelt.	ingebouwd	

Reageren: als het misgaat

	Status	Datum	Verantwoordelijke
☐	Incidentplan Wie belt wie, wat wordt gemeld aan het CCB binnen 24 en 72 uur. Een A4 volstaat voor Basic; leg het in de kluis.	uw beleid	
☐	Analyse: wat is er gebeurd Loginlogboek plus bewijsketen reconstrueren in minuten wie welk bestand deelde of opende.	ingebouwd	
☐	Beheersing Sessies beëindigen, account uitschakelen, wachtwoord resetten, bewaarplicht op betrokken bestanden.	ingebouwd	
☐	Communicatie en melding De export levert de feiten voor de melding; het melden zelf en de communicatie met betrokkenen doet u.	deels	

Herstellen: weer aan het werk

	Status	Datum	Verantwoordelijke
☐	Herstel uit back-up Zelf te herstellen met uw eigen sleutel, zonder ticket bij een leverancier.	ingebouwd	
☐	Herstelplan en test Documenteer wie herstelt, waar de sleutel ligt en hoe lang het mag duren. Test minstens jaarlijks.	deels	
☐	Lessen en verbetering Na een incident: wat passen we aan in beleid en instellingen? De compliance-score toont meteen het effect.	uw beleid	

