Stap voor stap naar veilige digitale informatie

Normenkader IBP voor het onderwijs

Het onderwijs digitaliseert in hoog tempo. Dat betekent ook meer dreigingen en privacyrisico's: phishing e-mails, ransomware en cyberaanvallen. Daarom werkt de onderwijssector toe naar één kader voor digitaal veilig onderwijs, het Normenkader Informatiebeveiliging en Privacy. Het berust op twee pijlers: informatiebeveliging en privacy. Hieronder gaan we specifiek in op de eerste pijler. Voor de twee andere pijlers kunt u terecht op deze pagina van Kennisnet.

Domeinen en normen voor betrouwbare informatiebeveiliging

De pijler Informatiebeveiliging is verdeeld in vijftien domeinen. Elk domein beschrijft een aantal normen om uw school optimaal te beschermen tegen digitale dreigingen van binnen en buiten uw organisatie. Door de normen toe te passen, beschermt u uw systemen – en dus uw onderwijs – tegen uitval, ongeoorloofde toegang en verstoringen. Gebeurt het toch? Dan bent u voorbereid en weet u wat u te doen staat.

De optelsom van alle domeinen biedt een goed uitgangspunt voor het opzetten van betrouwbare informatiebeveiliging. Hier lichten we er drie uit: Securitymanagement, Personeelsbeheer en incident- en problemmanagement.

De technische kant: securitymanagement

Dit domein omvat dertien normen die vooral gaan over de meer technische kant van informatie-beveiliging. Zo zijn er normen voor een betrouwbaar beveiligd netwerk maar ook voor het beheer van bedreigingen en kwetsbaarheden. Bij elkaar opgeteld zorgen de normen ervoor dat u risico's op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening zoveel mogelijk kunt signaleren en mitigeren. Bijvoorbeeld als u te maken krijgt met phishing en malware, of als de borging van informatiebeveiliging bij mobiele apparaten in het geding is.

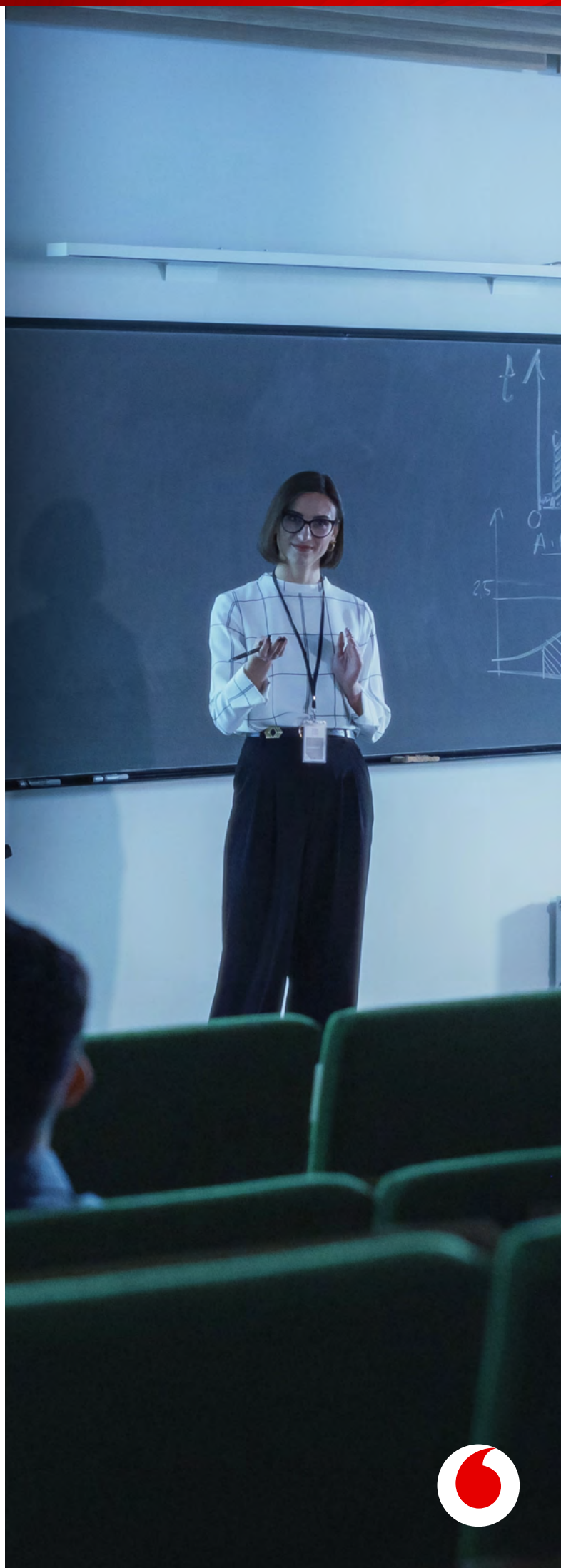
Voorbeeld van een belangrijke norm

Netwerkbeveiliging (norm SM.11)
Beveiligingstechnieken en bijbehorende beheerprocedures, zoals firewalls, beveiligingsapparatuur, netwerksegmentatie en inbraakdetectie, worden gebruikt voor het autoriseren van toegangs- en besturingsinformatiestromen van en naar netwerken. Er wordt gebruikgemaakt van best practices op dit gebied (bijvoorbeeld NCSC, ISO/IEC, ITSec).

Mobiele apparaten en telewerken (norm SM.03)
Informatiebeveiliging wordt geborgd bij het gebruik van mobiele apparaten en telewerkfaciliteiten. Mobile Device Management, versleuteling en bescherming tegen malware zijn aanwezig om de risico's te beperken.

Testen, inspectie en toezicht beveiliging (norm SM.05)
Implementatie van IT-beveiliging wordt proactief getest en bewaakt. IT-beveiliging wordt regelmatig getoetst om ervoor te zorgen dat de door de organisatie goedgekeurde baseline voor informatiebeveiliging wordt gehandhaafd. Een logen bewakingsfunctie maakt vroegtijdige preventie en detectie mogelijk en daardoor tijdige rapportage van ongebruikelijke en/of abnormale activiteiten.

Threat- en vulnerabilitymanagement (norm SM.07)
Er is een proces voor threat- en vulnerabilitymanagement ingevoerd om bedreigingen te identificeren en kwetsbaarheden tijdig te detecteren en te verhelpen. Het gaat hierbij om kwetsbaarheden die kunnen leiden tot een verslechtering van de prestaties van of een aanval op bedrijfsmiddelen. Welke aanvalsvectoren cybercriminelen gebruiken, wordt ook beschouwd en er worden maatregelen genomen om blootstelling te verminderen.



De hele cyclus van personeelsbeheer

De normen in dit domein hebben betrekking op alle medewerkers van de school. Van werving en doorstroming tot het moment van uit dienst gaan. Invallers, die vaak op korte termijn worden ingeschakeld en niet altijd lang blijven, vormen een extra uitdaging en vergroten de kwetsbaarheid op het gebied van informatiebeveiliging. Daarnaast is het van belang om de kennis over informatiebeveiliging te borgen en up-to-date te houden. Op die manier blijft de continuïteit van het onderwijs gewaarborgd wanneer medewerkers in een cruciale functie vertrekken.

Voorbeeld van een belangrijke norm

Bewustwording informatiebeveiliging (norm HR.06)
Er is een bewustwordingsprogramma om gebruikers bewust te maken van hun verantwoordelijkheid om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie(middelen) te beschermen.

Wat kunt u doen voor meer veiligheid?

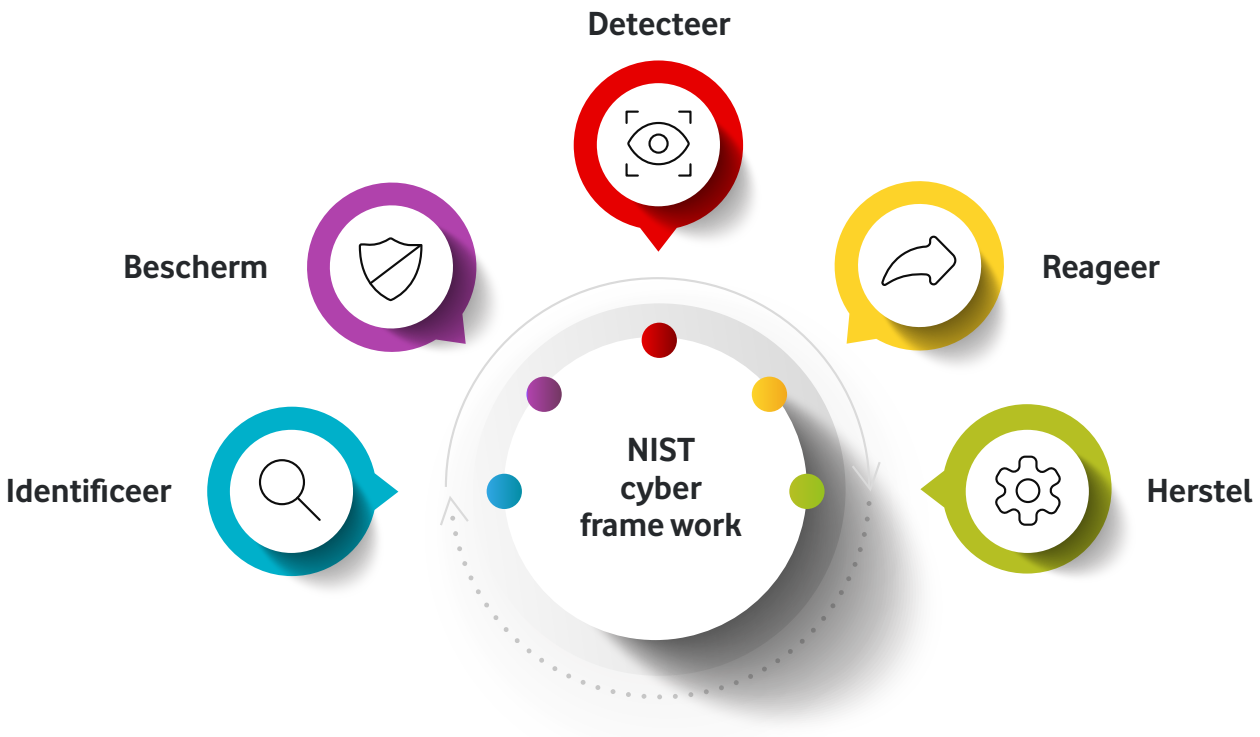
Bij de beveiliging van informatie spelen uiteenlopende vragen. Hoe lost u zo snel mogelijk verstoringen in de continuïteit op? Hoe detecteert u beveiligingsincidenten sneller en hoe pakt u ze aan? En: wat zijn de onderliggende oorzaken en hoe kunt u ze analyseren om het probleem structureel op te lossen? Het NIST Cybersecurity Framework biedt houvast: **identificeer, bescherm, detecteer, reageer en herstel.**

Identificeer hulp voor gebruikers
Help uw medewerkers. Maak ze bewust van de gevaren in de digitale wereld door ze te trainen, bijvoorbeeld om phishing via e-mails en socialmediaplatformen te leren herkennen. Cybercriminelen gaan zelfs zo ver dat medewerkers worden gechanteerd als ze geen informatie verstrekken. (norm. HR.06)
Lees meer over Vodafone Security Awareness >

80% van de gemelde cyberindicenten zijn phishingaanvallen. Met onze Phishing Awareness Service verkleint u de dreiging. U krijgt inzicht in het risico dat uw organisatie loopt, zodat u gericht actie kunt ondernemen en bewustwording bij medewerkers kunt vergroten. (norm. HR.06)
Lees meer over Vodafone Phishing Awareness >

Bescherm uw apparaten
Beheer uw apparaten op afstand om uw infrastructuur en medewerkers te beveiligen. Laat de apparaten voortdurend scannen en altijd veilig koppelen aan internet. Wij helpen u graag met tools om de toegang tot uw netwerk en de data in de cloud en in de organisatie te beveiligen. (norm SM.03)
Lees meer over Vodafone Secure Device Manager >

Wilt u mobiel werken mogelijk maken voor uw organisatie? En bijvoorbeeld een BYOD-strategie implementeren? Daar komt veel bij kijken. Zo is het cruciaal om mobiele toestellen – die steeds meer gevoelige en bedrijfskritieke informatie bevatten – te beveiligen tegen bedreigingen. (norm SM.03)
Lees meer over Lookout Mobile Security >



Als de kwetsbaarheid van systemen en netwerken niet wordt bewaakt, worden ze een makkelijk doelwit. Met onze Vulnerability Assessment Service geven we u inzicht in kwetsbaarheden in uw IT-infrastructuur en de mate van hun dreiging, zodat u gericht actie kunt ondernemen. (norm SM.07)
Lees meer over Vodafone Vulnerability Service >

Bescherm uw netwerk
Zet Local Area Networks (LANs) in voor campusbeveiliging en netwerken met hoge snelheid, Software-Defined Wide Area Networks (SD-WAN) voor veilige, intelligente en kosteneffectieve connectiviteit met meerdere campussen en clouds. (norm SM.11)
Lees meer over LAN's en SD-WAN >

Een DDoS-aanval (Distributed Denial-of-Service) overspoelt uw netwerk, server of website met internetverkeer. In het onderwijs kunnen DDoS-aanvallen aanzienlijke downtime veroorzaken, waardoor studenten en docenten geen toegang hebben tot online leerplatforms, e-mails of administratieve systemen. (norm SM.11)
Lees meer over Vodafone Anti-DDoS >

Bescherm uw cloud
Hoe sterk is uw toegangscontrole? Worden privacyregels nageleefd? Begin met onze Penetration Testing Service. Een professionele ethische hacker laat u ervaren hoe een aanvaller het aanpakt, wat de mogelijke impact is van kwetsbaarheden in uw IT-infrastructuur en hoe u uw beveiliging kunt verbeteren. (norm SM.05)
Lees meer over Vodafone Penetration Testing Service >

SASE (Secure Access Service Edge) helpt u gegevens te beschermen door beveiligingsbeleid af te dwingen, zoals veilige webgateways, zero-trusttoegang en encryptie. Cruciaal, nu steeds meer onderwijs-instellingen hun activiteiten naar de cloud verplaatsen. (norm SM.11)
Lees mere over Secure Access Service Edge >

Detecteer, reageer en herstel
Ook voor de laatste drie van de vijf NIST-speerpunten – detecteren, reageren en herstellen – zijn goede oplossingen beschikbaar. Wilt u cyberdreigingen detecteren? Sneller reageren op een incident? Of beschikken over de tools om te interveniëren? Managed Extended Detection & Response (MxDR) biedt u 24 uur per dag realtime detectie van en reactie op cyberrisico's. (norm IM.01-04)

Onze systemen en experts analyseren continu uw IT-systemen. Zij waarschuwen u vrijwel realtime over cyberaanvallen, informeren u vroegtijdig over cyberrisico's en bezorgen u de juiste rapportages en adviezen om structureel actie te ondernemen om uw organisatie weerbaar te maken tegen cybercriminelen.
Lees meer over Managed Extended Detection & Response >

Zet de volgende stap

Meer weten over het normenkader voor informatiebeveiliging? Lees deze pagina. En wilt u actief met dit thema aan de slag? Dan kunt u de volgende stappen aanhouden:

- Voorbereiding: leg de basis voor beveiligingsmaatregelen.
- Risicomanagement: pak de meest kritieke beveiligingsrisico's aan.
- Voortgang: implementeer de beveiligingsnormen in volgorde van prioriteit.
- Integratie: versterk de beveiliging door aanvullende normen te integreren.
- Voltooiing: rond de implementatie af voor alomvattende beveiliging.

U staat er niet alleen voor

Vodafone Business helpt mensen, locaties en dingen op een veilige manier te verbinden. Dat begint bij de bewustwording van de gebruiker en loopt via de beveiliging van toestellen en netwerk naar een veilig gebruik van apps en data. Zo zijn alle gevoelige gegevens in de cloud én de apparatuur die uw medewerkers op kantoor of thuis gebruiken altijd optimaal beveiligd.

Vodafone Business
Together we can