



Whitepaper

Tips voor het bouwen van een veilige leeromgeving

De uitdagingen voor digitale veiligheid in de onderwijsmarkt

In de snel evoluerende digitale wereld is het waarborgen van de veiligheid en gebruiksvriendelijkheid van de schoolomgeving van cruciaal belang. Digitale veiligheid is niet langer een optie, maar een absolute noodzaak, ook voor onderwijsinstellingen. Scholen, groot of klein, worden niet gespaard van de dreiging van ransomware.

In onze digitale wereld worden bijna 75% van de incidenten op onderwijsinstellingen veroorzaakt door niet-cyber gerelateerde problemen, zoals onbedoelde aanvallen en fouten in het gebruik van e-mail.

Vooraf het onterecht delen van gevoelige informatie, zoals gezondheidsgegevens van leerlingen, kan desastreuze gevolgen hebben. Met de groeiende ouderbetrokkenheid en de opkomst van afstandsonderwijs is het van cruciaal belang om het onderwijspersoneel uit te rusten met technologie die compliance en de juiste behandeling van gegevens waarborgt.

Leerlingen, ouders, collega's en andere belanghebbenden communiceren dagelijks verspreid over verschillende locaties. E-mail, hoewel betrouwbaar, biedt geen garantie voor gegevensbescherming. Alternatieve communicatieplatforms missen vaak gebruiksvriendelijkheid en worden daardoor niet volledig gebruikt.

Verhoog de digitale veiligheid in het basisonderwijs, voortgezet onderwijs en vervolgonderwijs

Scholen in het primair en voortgezet onderwijs blijken vaak digitaal kwetsbaar te zijn. Het misleidende idee van “wij zijn maar een kleine school in een kleine gemeente, ons zal niets overkomen” is een valkuil die vermeden moet worden. Gezien de persoonsgegevens die scholen beheren, dragen zij een grote verantwoordelijkheid voor zorgvuldige gegevensverwerking. Dit geldt des te meer omdat privacy kwesties bij jongeren en kinderen gevoeliger liggen dan bij volwassenen.



Helaas zien we dat privacyoverwegingen soms leiden tot terughoudendheid bij het gebruik van slimme technologieën. Angst voor datadiefstal of onbekendheid met de werking van digitale oplossingen kan ertoe leiden dat deze niet volledig worden benut.

Een veilige toekomst: investeren in digitale veiligheid en privacy

Het ministerie van Onderwijs, Cultuur en Wetenschappen erkent de urgentie van het verbeteren van de digitale veiligheid in het primair en voortgezet onderwijs. In een recente brief aan de Tweede Kamer is een ambitieus plan gepresenteerd dat niet alleen investeringen en beleidsmaatregelen omvat, maar ook specifieke afspraken met toonaangevende softwareleveranciers. Het onderwijs wordt beschouwd als een prioritaire sector, aangezien het steeds vaker het doelwit is van cyberaanvallen. Het ministerie van OCW¹ zal de komende jaren 6 miljoen euro toewijzen aan nieuwe maatregelen om de digitale veiligheid te versterken.

¹<https://www.rijksoverheid.nl/ministeries/ministerie-van-onderwijs-cultuur-en-wetenschap/documenten/kamerstukken/2022/07/14/verhogen-digitale-veiligheid-onderwijs-en-onderzoek>



Bouw samen aan een veilige digitale leeromgeving

IT/ICT coördinatoren spelen een cruciale rol in het waarborgen van privacy en beveiliging op school. Maar hoe is het op dit moment gesteld met de digitale veiligheid? Maakt jouw organisatie al gebruik van geavanceerde digitale oplossingen of software met ingebouwde compliance-oplossingen?

Hier zijn enkele praktische tips die je direct kunt toepassen:

Tip 1: Beveiliging met Multi Factor Authentication

Beveilig alle schoolapplicaties met Multi Factor Authentication, een minimale tweestapsverificatie. Dit vermindert aanzienlijk de kans op digitale bedreigingen, vooral omdat de meeste cyberaanvallen via e-mail plaatsvinden. Hoe meer leerlingen en leerkrachten Multi Factor Authentication instellen, hoe kleiner de kans op ransomware-aanvallen waarbij losgeld moet worden betaald. Conditional Access kan ook worden gebruikt om de gebruiksvriendelijkheid hoog te houden, waarbij leerlingen niet constant hun telefoon hoeven te raadplegen voor bevestiging.

Tip 2: Back-ups met veilige Cloud diensten

Denk altijd aan het maken van back-ups. Gebruik veilige clouddiensten zoals Microsoft OneDrive of Google Cloud om kopieën van het schoolwerk van leerlingen veilig te bewaren. Controleer regelmatig of de back-ups correct worden uitgevoerd en of je in staat bent om de data netjes terug te zetten. Probeer dit rustig uit met een testbestandje voordat het echt nodig is.



Tip 3: Wees alert op Phishing aanvallen

Wees alert op phishingaanvallen, ook voor leerlingen. Leerlingen kunnen slachtoffer worden van internetfraude, zoals phishing, waarbij ze naar valse websites worden gelokt om persoonlijke informatie achter te laten. Waarschuw leerlingen voor de gevaren van phishing, zowel op e-mail als op platforms zoals WhatsApp. Moedig hen aan om verdachte berichten te verifiëren bij de echte afzender.

Tip 4: Gebruik een oplossing voor het veilig versturen of ontvangen van bestanden

Stel al het onderwijzend personeel in staat om efficiënt en zonder platformwisselingen te communiceren. Maak het gemakkelijk voor iedereen. Dagelijkse taken, zoals het delen van grote bestanden tussen teams en ouders, zoals rapporten, aanwezigheids- en registratiegegevens, gezondheids- en veiligheidsinformatie, moet eenvoudig te realiseren zijn.

Over mSafe

mSafe biedt een oplossing met een slimme, AVG proof, gebruiksvriendelijke oplossing afgestemd op uitdagingen in het onderwijs. Onderwijspersoneel moet moeiteloos kunnen communiceren zonder voortdurend tussen verschillende platforms te schakelen. Essentiële functies zijn onder meer de mogelijkheid om grote bestanden te delen, de identiteit van de ontvanger te verifiëren en controle te behouden over verzonden berichten. Daarnaast kunnen medewerkers veilig digitaal ondertekenen.

Onze oplossing is al binnen één week, organisatie breed, te implementeren. Dus geen ingewikkeld gedoe maar gewoon een oplossing die snel en gemakkelijk te gebruiken is.

Zelf ervaren hoe eenvoudig onze oplossing werkt? [Maak nu een gratis account aan.](#)