Naar een veiligere, hybride onderwijs-omgeving

breens network

Waar het mis ging

Een beknopt overzicht van openbaar gemaakte, geslaagde cyberaanvallen op onderwijsinstellingen. Dit is geen uitputtende opsomming, maar de voorbeelden maken wel duidelijk dat er urgent oplossingen nodig zijn.

3,4 Procent van de Nederlandse jongeren is wel eens binnengedrongen in een digitaal onderwijssysteem. Hierdoor kunnen in sommige gevallen cijfers worden veranderd, roosters worden aangepast en kan er worden gefraudeerd met afwezigheid. Dat blijkt uit onderzoek van Veiliginternetten.nl onder ruim 1000 jongeren tussen de 12 en 18 jaar.

Het Staring College in Lochem en Borculo is slachtoffer geworden van een cyberaanval. De onderwijsinstelling blijft vanwege schade aan de systemen maandag dicht, ook online worden geen lessen gegeven. Het bestuur van het Staring College in Lochem en Borculo heeft losgeld betaald om van de internetcriminelen af te komen. Lees het bericht in NRC.

De Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) is gehackt door DoppelPaymer, een bekende en vrij agressieve groep criminelen die met gijzelsoftware organisaties afperst. De criminelen zouden miljoenen euro's aan losgeld vragen. Lees het bericht in De Volkskrant.

De Universiteit en Hogeschool van Amsterdam hebben te maken met een aanval op hun ict-systemen. Dat melden de onderwijsinstellingen op de servicepagina's van hun website. Wat de aanval behelst, wat de omvang is en wie erachter zit is op dit moment allemaal onduidelijk.

Hogeschool Inholland is het slachtoffer geworden van een dataroof. Hackers hebben op internetfora de persoonlijke gegevens van 56.000 studenten en medewerkers aangeboden. Lees het bericht in het Parool.

De Universiteit Maastricht heeft bijna twee ton aan losgeld betaald aan hackers die de universitaire computer-systemen kort voor Kerstmis 2019 via een cyberaanval (ransomware) platlegden. Lees het bericht op RTL.

Geen onderwijsinstelling, niettemin spraakmakend: Gemeente Hof van Twente trekt twee en een half jaar uit om de ict-infrastructuur opnieuw op te bouwen na een ransomware-aanval begin december 2020. De Overijsselse gemeente benadrukt dat de normale dienstverlening weer loopt, al gaat er als gevolg van de hack nog veel handmatig. Lees het bericht op Computable.

De privégegevens van afgestudeerden aan de TU Delft en Universiteit Utrecht zijn in handen gekomen van cybercriminelen. De onderwijsinstellingen zijn hierover op de hoogte gebracht door softwarebedrijf Blackbaud, dat back-ups van de universiteiten op de server had staan. Lees het bericht in Trouw.

Pornobeelden en racistische uitlatingen tijdens een digitale les. Dat is de nachtmerrie van elke docent. Het gebeurde vanochtend bij het Erasmus College uit Zoetermeer via video-app Zoom. De onderwijsinstelling is per direct gestopt met het gebruik van Zoom. Lees het bericht in het AD.

De stichting Limburgs Voortgezet Onderwijs (LVO) is getroffen door een computervirus. Ongeveer 26.000 scholieren en leraren kunnen niet werken op de computers. Alle 23 scholen die onder de stichting vallen, zijn getroffen. Dat melden De Limburger en 1Limburg.

De digitale systemen van de middelbare scholen op Zeeuws-Vlaanderen zijn al sinds eind 2020 het doelwit van een reeks DDoS-aanvallen. Dat leidt tot storingen en haperingen in die systemen, waardoor online lesgeven wordt bemoeilijkt. Hierbij worden doelbewust de systemen van de scholen zelf én door de scholen gebruikte systemen van derden aangevallen. Zo meldt Omroep Zeeland.

In december 2020 moest de Radboud Universiteit Nijmegen een tentamen afblazen vanwege herhaalde DDoS-aanvallen. Lees het bericht in het Algemeen Dagblad.

Voorwoord

Allereerst mijn bewondering voor al diegenen die het in het afgelopen jaar mogelijk hebben gemaakt om een hybride leeromgeving neer te zetten. Covid-19 heeft ook besturen in het voortgezet en hoger onderwijs voor het blok gezet. Toch is onderwijs doorgegaan, dankzij de tomeloze inzet van docenten en IT-afdelingen. Nederland beschikt over hoogwaardige, gedigitaliseerde processen en een fijnmazige communicatie-infrastructuur. De scholen hebben dit goed weten te gebruiken.

Toch lezen we regelmatig dat onderwijsinstellingen te maken hebben met geslaagde cyber-aanvallen. Dit zou erop kunnen wijzen dat bij bestuurders van onderwijsinstellingen mogelijk nog te weinig oog is voor het adequaat, duurzaam beschermen van de digitale infrastructuur en de (vaak minderjarige) gebruikers daarvan tegen cybercriminaliteit. Daarom heeft Breens Network opdracht gegeven aan onderzoeksbureau Kantar om in kaart te brengen hoe het zit met het aanbieden van een veilige (digitale) leeromgeving. Ondervraagd zijn onderwijsbestuurders en IT'ers die binnen het onderwijs werken. De resultaten zijn ronduit verontrustend. De vraag dringt zich op of het onderwijs zich wel voldoende bewust is van de risico's. Niet alleen vanuit het perspectief van de onderwijs-instelling, maar ook die van de bestuurder, en of men weet wat er kan en moet worden gedaan om de risico's te beperken. Als blijkt dat ca. 60% van de onderwijsinstellingen 5% of minder van het IT-budget uitgeeft aan privacy & security dan moet het antwoord op die vraag (helaas) 'nee' zijn.

Onderwijsinstellingen lopen voortdurend het risico dat data worden gestolen en misbruikt. Criminelen kunnen het onderwijs platleggen en onderwijsinstellingen en hun bestuurders riskeren bovendien forse reputatieschade. Zij immers zijn verantwoordelijk voor het realiseren van een duurzame, veilige digitale omgeving. Uit het onderzoek blijkt dat er veel gesproken wordt over IT-security, maar vaak alleen binnen de IT-afdelingen. Wat ontbreekt is daadwerkelijk, bestuurlijk inhoud geven aan de thematiek, er actie op ondernemen, de situatie monitoren en er in openheid en transparantie over rapporteren. Er is een discrepantie tussen 'zeggen' en 'doen', tussen bestuurlijke verantwoordelijkheid nemen en verantwoordelijkheid delegeren.

Een veilige digitale onderwijsomgeving is niet iets dat primair op het bordje van de IT-afdeling ligt. De verantwoordelijkheid ligt duidelijk in de eerste plaats bij het bestuur van de onderwijs-instelling en de bestuurders persoonlijk. Alleen de uitvoering van de noodzakelijke maatregelen kan dan door een IT-afdeling worden verzorgd.

De maatschappij en dus de overheid heeft baat bij een veilige hybride onderwijsomgeving, zeker in het digitale kennisland dat Nederland wil zijn. De politiek zal zich nadrukkelijker met deze kwestie bezig moeten houden. Het is een zaak die ons allen aangaat.

Breens Network biedt deze whitepaper aan om duidelijk te maken waarom dit onderwerp zo belangrijk is. Tegelijkertijd willen we handvatten geven om te komen tot een verantwoorde, veilige (hybride) leeromgeving. Om dat uiteindelijke doel te helpen realiseren, gaan we dan ook graag het maatschappelijk debat aan!

Geert-Jan van der Snoek,
CEO Breens Network

Managementsamenvatting

De digitalisering in het onderwijs neemt in snel tempo toe. De lockdowns als gevolg van het coronavirus hebben de noodzaak daarvan nog eens extra onderstreept. De cyberdreigingen die met deze digitalisering gepaard gaan, baren zorgen of zouden dat ten minste moeten doen. Hoe groot is de dreiging van cybercriminaliteit en hoe wapenen onderwijsinstellingen zich hiertegen? Onderzoeksbureau Kantar bracht die thematiek in kaart. In deze whitepaper worden de resultaten gepresenteerd, gekoppeld aan een visie op digitalisering in het onderwijs. De paper geeft daartoe concrete handvaten mee voor besturen van onderwijsinstellingen en overwegingen voor de politiek die bij de noodzakelijke beleidsvorming gebruikt kunnen worden.

Het onderwijsveld is lucratief voor criminelen. Na de gezondheidszorg bevinden zich in de digitale onderwijssystemen de meeste bruikbare gegevens: persoonsgegevens, financiële data, informatie over (geestelijke) gezondheid en kennisniveau, data van onderzoeksprojecten, etc. De meeste cyberaanvallen vinden daarom momenteel in het onderwijs plaats.

De gevolgen hiervan voor het onderwijs zijn groot: identiteitsfraude, tijd- en energieverlies, verminderde bereikbaarheid, extra beveiligingskosten, verlies van continuïteit en de daaruit voortvloeiende bedreiging van leerresultaten, herstelkosten, reputatieschade, verlies van gegevens en de kosten van betaald losgeld bij geslaagde aanvallen.

Bij 60 % van alle onderwijsinstellingen gaat 5 % of minder van het IT-budget naar beveiliging.

Het bestuur van een onderwijsinstelling is verantwoordelijk voor digitale veiligheid, maar die bestuursorganen zijn hier vaak onvoldoende van doordrongen of op toegerust. Zo gaat bij ca. 60 % van alle onderwijsinstellingen 5 % of minder van het IT-budget naar beveiliging (als dit percentage al bekend is, want vaak wordt het niet uitgesplitst). Dat is een enorm verschil met de 25% budget-besteding die in het bedrijfsleven gebruikelijk is.

Er is een groter besef van verantwoordelijkheid nodig bij de bestuurders van onderwijsinstellingen waar het gaat om een dataveilige omgeving. Niet alleen voor bescherming en preventie, maar ook vanwege de aansprakelijkheid - en consequenties - als er wél iets mis gaat. Mocht de continuïteit van onderwijs zijn onderbroken door bijvoorbeeld een DDoS-aanval, ransomware of erger, dan komt het bestuur van de onderwijsinstelling zijn contract met studenten of leerlingen niet na. Gedupeerden kunnen het bestuur van een onderwijsinstelling hiervoor aansprakelijk stellen.

Wat kan de overheid doen?

Het Rijk kan, naar analogie van de duurzaamheidsparagraaf die wordt geëist bij bedrijven, van besturen van onderwijsinstellingen eisen dat zij in jaarverslagen beschrijven welke maatregelen zij hebben genomen om een duurzame, cyberveilige leeromgeving te creëren. Die besturen zouden zich daarbij moeten kunnen baseren op een door het Rijk te ontwikkelen raamwerk dat aangeeft waar een cyberveilige onderwijsinstelling aan móet voldoen. Dit kan meewegen in het budget dat een onderwijsinstelling van het Rijk ontvangt. Het raamwerk zou het Rijk moeten opstellen in nauwe samenspraak met het onderwijsveld en het bedrijfsleven (de securityspecialisten en –dienstverleners). De uitvoering daarvan zou in handen gelegd kunnen worden van de onafhankelijke accountants of bijv. in het ingeval van universiteiten bij SURF.

Een dergelijke verplichte, te controleren IT-paragraaf in het wettelijk verplichte jaarverslag leidt tot meer bewustzijn bij onderwijsinstellingen en -bestuurders, wat een essentiële voorwaarde is voor cyberveilige leeromgevingen. Het is belangrijk dat onderwijsbestuurders daarbij de noodzakelijke handvatten aangereikt krijgen en geïnformeerd worden over de juiste maatregelen. Deze paper geeft daartoe een aanzet.

Deze whitepaper is als volgt opgebouwd.

1: Beschrijft de toenemende dreiging van cybercriminaliteit.
2: Verklaart waarom onderwijs zo aantrekkelijk is voor cybercriminelen.
3: Geeft een kort overzicht van de meeste voorkomende dreigingen.
4: Licht toe wat gevolgen zijn van geslaagde aanvallen voor onderwijsinstellingen.
5: Schetst de stand van zaken rondom cyberveiligheid in het onderwijs.
6: Legt uit wie verantwoordelijk is voor cyberveiligheid.
7: Beschrijft wat de politiek en de overheid kunnen doen tegen cyberdreigingen.
8: Beschrijft hoe bewustzijn kan worden gecreëerd binnen onderwijsinstellingen.
9: Benoemt concrete stappen die besturen van onderwijsinstellingen kunnen zetten om cyberaanvallen te voorkomen.

Deel 2: Een onverkorte rapportage van het onderzoek dat door Kantar in opdracht van Breens Network is uitgevoerd, inclusief de onderzoeksverantwoording.

Men heeft maar half in de gaten wat de impact van het stelen van identiteit teweeg brengt. Het onderwijs grossiert in persoonsgegevens.

Op koers naar cyberramp

1

Onderwijsinstellingen stevenen af op cyberramp, zo kopte Computable op 20 november 2020 in een artikel 'Onderwijsinstellingen stevenen af op cyberramp Alarmerende situatie vraagt om onmiddellijke actie') over de risico's in het onderwijs. "De publieke sector is altijd al een populair doelwit geweest van cybercriminelen, waarbij vooral de onderwijssector het moet ontgelden. De laatste jaren nemen de frequentie, het niveau en de kosten van cyberaanvallen tegen laatstgenoemde sector schrikbarend toe. En dat hoeft niet te verbazen."

Het beeld dat Computable schetst, wordt ook onderstreept door het onderzoek van Kantar (zie deel 2 van deze whitepaper, blz. 29 voor de onderzoeksverantwoording), dat wil laten zien welke bedreigingen er zijn en welke mogelijke oplossingen voorhanden zijn. Want dat er nog werk aan de winkel is, is duidelijk.

Verdere digitalisering van het onderwijs verdient een stevigere rol in discussies en daarom een plaats op de formatietafel. Nederland wil immers een kennisland zijn. Goed onderwijs is daarvoor een vereiste. Nederland scoort in de top 5 waar het gaat om de inhoud van het onderwijs, Nederland staat 5e in digitale skills en houdt de curricula actueel. "Op basis van de beschikbare gegevens behoren Nederland, Denemarken, Zwitserland en Finland tot de beter voorbereide landen, die zich inspannen om de leerplannen van scholen relevant en actueel te houden", aldus het World Economic Forum (lees: 'Global Competitiveness Report Special Edition 2020: How Countries are Performing on the Road to Recovery' van het WEF). Behoud van die positie is het beschermen waard!

Formatiebesprekingen

Tijdens de formatiebesprekingen ligt de 'Ambtelijke verkenning beleidsopties voor groei n.a.v. motie Wiersma' op tafel. Daarin wordt beschreven hoe het groeivermogen van de Nederlandse economie op een hoger peil is te brengen. Beter onderwijs speelt hierin een belangrijke rol. Evenals verdere digitalisering. Volgens de notitie zijn tijdens de pandemie (digitale) innovaties binnen het onderwijs versneld, zoals het aanbieden van onderwijs op afstand. "Daarbij blijkt wel dat de kansen die digitalisering biedt voor de kwaliteit van het onderwijs nog onvoldoende worden benut", aldus het Ministerie van Economische Zaken en Klimaat.

De kansen die digitalisering biedt voor de kwaliteit van het onderwijs worden nog onvoldoende benut.

Wie de uitkomsten van het Kantar-onderzoek bestudeert, komt eerder tot de conclusie dat we moeten beginnen met dijkversterkingen.

Er zou meer aandacht moeten zijn voor leermiddelen als augmented reality, learning analytics en serious games. “Taken als lesvoorbereiding en het nakijken van toetsen en tentamens kunnen (deels) door ICT worden overgenomen. Dit verlaagt de werkdruk van docenten en vergroot de tijd voor begeleiding van leerlingen en studenten en andere waarde-toevoegende activiteiten. Het kan de docent in staat stellen om vaardigheden en kennis effectiever en motiverender over te dragen. Bijvoorbeeld door traditionele onderwijsvormen, zoals het hoorcollege, te verrijken met digitale onderwijsvormen.”

Ondanks de omvang van de notitie (70 pagina’s) komen de woorden IT-security en databeveiliging er niet in voor. Dat is verontrustend: toenemende digitalisering kan immers alleen veilig plaatsvinden, als dat hand in hand gaat met grotere aandacht voor IT-beveiliging. Dat blijkt echter een ondergeschoven kind

Dijkversterkingen

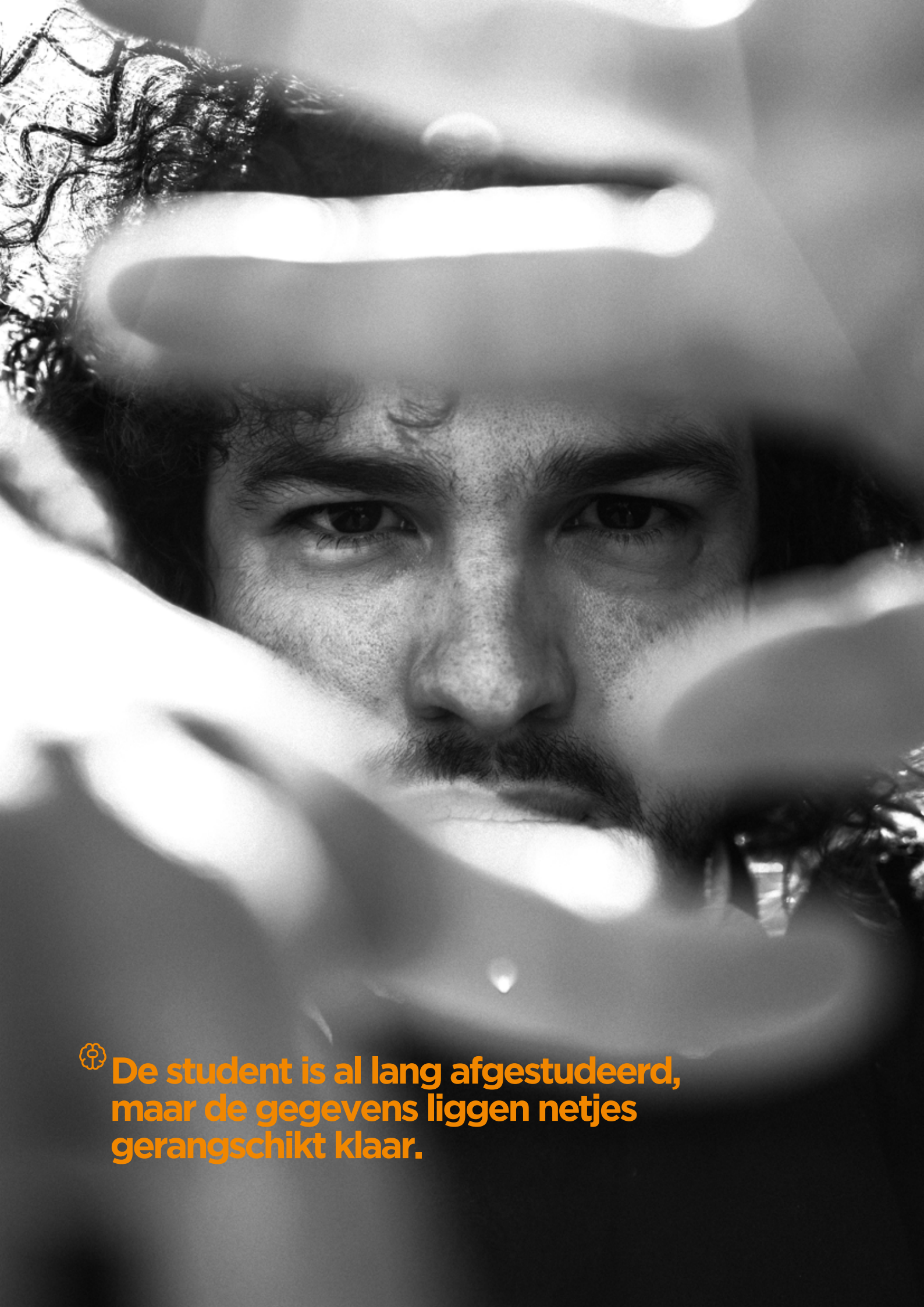
Uit het onderzoek van Kantar blijkt dat vier op de tien instellingen te maken hebben gehad met problemen op het gebied van IT-beveiliging. Overigens weet 7% niet of de onderwijsinstelling aanvallen te verduren heeft gehad. Het bestuur, de directie en evt. CIO meent vaker last te hebben van problemen (56%) dan de IT-medewerker (31%). Dit duidt erop dat de eerste groep niet goed weet wat er gebeurt binnen de systemen, gezien de afwijkende inschatting van de IT-medewerkers die per definitie ‘dichter bij het vuur’ zitten.

En dat het niet om triviale zaken gaat, blijkt een recente studie van de University of Maryland: Hackers worden steeds professioneler, ze vallen nu elke 39 seconden aan. Dat gebeurt wereldwijd. Uit de ‘Microsoft-sensor’ blijkt dat Nederland in absolute aantallen weliswaar onderdoet voor bijvoorbeeld de VS of China, maar verhoudingsgewijs een interessant land is voor hackers. Kennelijk omdat er ‘toegang’ is tot aantrekkelijke gegevens van een bevolking met een bovengemiddeld inkomen.

Om met Jet de Ranitz, voorzitter raad van bestuur SURF, te spreken:

> Ontwikkelingen op het gebied van cyberweerbaarheid zijn als positief te beschouwen. Maar dit cyberdreigingsbeeld geeft tegelijk ook aan dat er nog steeds reden is tot verhoogde dijkbewaking.

De vraag is of er inderdaad behoefte is aan verhoogde dijkbewaking. Wie de uitkomsten van het door Kantar-uitgevoerde onderzoek bestudeert, komt eerder tot de conclusie dat we nu echt eerst moeten beginnen met dijkversterkingen.



De student is al lang afgestudeerd, maar de gegevens liggen netjes gerangschikt klaar.

Onderwijsdata zijn aantrekkelijk

2

Er zijn vijf sectoren die het meest last hebben van digi-inbrekers: het midden- en kleinbedrijf, de gezondheidszorg, overheidsorganen, energiebedrijven, en instellingen voor hoger onderwijs. Welk onderzoek je er ook bij pakt, onderwijs scoort hoog in de aanvalsplannen van hackers. Volgens Microsoft is 60 procent van alle aanvallen gericht op het onderwijs.

Een gegeven dat niet bekend blijkt binnen de onderwijssector. Daar denkt men dat vooral financiële instellingen het doelwit van hackers zijn: slechts 19 procent noemt onderwijs als primair doel. Men zou zich toch bewust moeten zijn van de aantrekkelijkheid van de eigen sector om op die manier minimaal begrip te hebben voor de interesse in het onderwijs van de kant van hackers.

Waarom is het onderwijs aantrekkelijk?

Het is niet vreemd dat juist onderwijsinstellingen zo in trek zijn. Uit het Data Breach Investigation Report 2020 van Verizon blijkt dat 90 procent van alle aanvallen is bedoeld om geld te genereren, de overige 10 procent betreft industriële spionage. En je vangt geld als je interessante data weet te bemachtigen.

Ga maar eens na wat voor gegevens onderwijsinstellingen allemaal beheren: dat begint met het leerling/studentendossier:

- gegevens over in- en uitschrijving;
- gegevens over afwezigheid;
- adresgegevens;
- gegevens die nodig zijn om te berekenen hoeveel geld de onderwijsinstelling krijgt;
- het onderwijskundig rapport;
- gegevens over de gezondheid van de leerling/student die nodig zijn voor speciale begeleiding of speciale voorzieningen;
- gegevens over de vorderingen en de resultaten van de leerling/student;
- verslagen van gesprekken met de ouders;
- resultaten van eventueel psychologisch onderzoek;
- onderzoeksresultaten binnen het wetenschappelijk onderwijs;
- (persoonlijke) gegevens van het personeel.

Dergelijke data zijn door te verkopen voor bijvoorbeeld identiteitsdiefstal of aan partijen die geïnteresseerd zijn in de kennis die binnen projecten is opgedaan.

Daarbij komt dat er bewaartermijnen gelden. Voor het leerling/studentendossier bijvoorbeeld een termijn van vijf jaar na de laatste inschrijving. De student is al lang afgestudeerd, maar de gegevens liggen netjes gerangschikt klaar. Niet voor niets richten aanvallers het vaakst hun pijlen op de educatieve sector. Volgens Microsoft vindt wereldwijd meer dan 60 procent van de cyber-aanvallen in de onderwijssector plaats (zie www.microsoft.com/en-us/wdsi/threats).

Uit de studie van Kantar blijkt dat betrokkenen uit het onderwijsveld het belang van 'hun' gegevens voor criminelen ernstig onderschatten. Zij weten niet dat onderwijs met stip op nummer 1 staat. Ter vergelijking: de helft van de respondenten denkt dat de financiële sector de meeste aanvallen te verduren krijgt, terwijl die sector in werkelijkheid met 5,6% de vierde plaats bezet.

Krappe IT-budgetten

Als het de hacker niet te doen is om het verhandelen van persoonlijke gegevens, dan kan hij altijd nog de onderwijsinstelling 'gijzelen'. Dat gebeurt wanneer ransomware wordt ingezet om gegevens te versleutelen, zodat ze niet langer bruikbaar zijn voor de rechtmatige eigenaar. Vervolgens eisen de hackers losgeld voor het opheffen van de versleuteling. In een variant op het gijzelen van gegevens, worden de systemen zelf dusdanig aangevallen dat het onderwijs in de knel komt. Na betaling worden de systemen weer vrijgegeven. Dat laatste gebeurt overigens niet altijd, zo blijkt uit The State of Ransomware 2020 van securityspecialist Sophos.

Er is, behalve de rijkdom aan data, nog een reden waarom scholen zo in trek zijn bij cyber-criminelen. Ook zij kiezen voor de weg van de minste weerstand. Zodra een inbreker tijdens zijn nachtelijke ronde een zwaarbewaakt huis (camera's, hond, speciale sloten) tegenkomt, is hij geneigd naar de buren te gaan die zich wat nonchalanter hebben verdedigd. Dat is in de digitale wereld niet anders.

Ook cybercriminelen kiezen voor de minste weerstand.

Rob Sanders, Lead Solutions Consultant bij OpenText (toonaangevend softwarebedrijf dat zich richt op databescherming), stelt vast dat juist in 2020 de pijlen van kwaadaardige hackers gericht zijn geweest op de gezondheidszorg en het onderwijs. "Heel snel moesten scholen onderwijs op afstand gaan regelen. Daar hebben criminelen gebruik van gemaakt. Uit ons Threat Report 2020 blijkt dat in 2020 maar liefst 700 procent meer aanvallen zijn gepleegd via het Remote Desktop Protocol, dat wordt gebruikt voor beheer van apparatuur op afstand. Hackers kiezen natuurlijk ook sectoren waarbij traditiegetrouw de IT-budgetten niet zo groot zijn. Daar valt het onderwijs ook onder."

Breed gamma van bedreigingen

3

Zonder een uitputtende lijst op te sommen van bedreigingen in het digitale domein, willen we hier toch even aandacht besteden aan een aantal veelgebruikte aanvalstechnieken, te beginnen met de meest voorkomende en ook meest spraakmakende: ransomware. Volgens IT-beveiligingsspecialist Sophos is, dankzij Covid-19, het onderwijs een slagveld geworden voor ransomware-aanvallen. Terwijl scholen zich het hoofd braken over online oplossingen voor continuering van de lessen, zagen criminelen hun kans schoon. Zij waren zich al snel bewust van mogelijkheden om de systemen binnen te dringen via studenten die op hun laptop contact hebben met de onderwijsinstelling.

Tegenwoordig maken cybercriminelen eerst een kopie van alle gegevens, zodat ze ook nog eens kunnen dreigen met openbaarmaking.

Ransomware blokkeert het gebruik van gegevens in een systeem door ze te versleutelen. Wie losgeld betaalt, krijgt de sleutel om alle data weer bruikbaar te maken. Voorheen gijzelden de criminelen alleen de getroffenen, tegenwoordig maken ze eerst een kopie van alle gegevens, zodat ze ook nog eens kunnen dreigen informatie openbaar maken als niet aan hun eisen wordt tegemoetgekomen.

Of ze nu betaalden of niet, slechts 29% van de slachtoffers wereldwijd kon na een aanval al hun versleutelde of geblokkeerde bestanden herstellen. De helft verloor ten minste enkele bestanden, 32% verloor een aanzienlijk deel, 18% verloor een klein aantal bestanden en 13% verloor bijna alle gegevens. Dit blijkt uit een recent onderzoek van Kaspersky.

Actie: Betaal geen losgeld als een apparaat is vergrendeld. Betaling van, in veel gevallen buitensporige bedragen aan losgeld, moedigt cybercriminelen alleen maar aan om door te gaan met hun praktijken. Neem in plaats daarvan contact op met de plaatselijke wetshandhavingsinstantie en meldt de aanval. Uit het eerder aangehaalde onderzoek van Sophos blijkt dat betaling van losgeld de totale kosten die gemoeid zijn met de ransomware-aanval verdubbelt.

- Probeer de naam van de ransomware Trojan te achterhalen. Deze informatie kan cybersecurity-experts helpen de dreiging te decoderen en toegang tot uw bestanden te herstellen.
- Klik niet op links in spam-mails of op onbekende websites en open geen e-mailbijlagen van afzenders die u niet vertrouwt.
- Steek nooit USB-sticks of andere verwijderbare opslagapparaten in uw computer als u niet weet waar ze vandaan komen.
- Maak zeer regelmatig een offline back-up. Controleer deze en ga na of herstellen (restore) het gewenste resultaat levert. Implementeer een Cloud Access Security Brokers (CASB) technologie, zoals Microsoft Cloud App Security (MCAS). Deze technologie geeft inzage in, grip op en controle over het gebruik van cloudapplicaties met data.

DDoS-aanvallen zijn een goede tweede: criminelen sturen extreem veel berichten naar een (web)server waardoor deze overbelast raakt en het opgeeft. Gevolg is dat het onderwijs stilvalt.

"In 2020 hebben we een aantal opvallende ontwikkelingen gezien. De DDoS-aanvallen werden complexer, krachtiger en duurden vooral een stuk langer in vergelijking met de aanvallen in 2019", aldus het 2020-jaarrapport van de Nationale Beheersorganisatie Internet Providers. De trend zet door; in het eerste kwartaal van 2021 waren er al meer aanvallen dan in dezelfde periode van 2020. De cijfers zijn afkomstig van de Nationale DDoS Wasstraat (NaWas). In december 2020 moest de Radboud Universiteit Nijmegen een tentamen afblazen vanwege herhaalde DDoS-aanvallen.

Actie: Verwijder software/diensten die niet meer worden gebruikt, zodat poorten niet onnodig open staan. Gebruik een firewall. Gebruik een Web Application Firewall voor de webservers. Beveilig de vertaling van domeinnaam naar IP-adres met DNSSEC.

Malware: schadelijke software die anderen de mogelijkheid geeft een computer op afstand te bedienen. Vaak na een phishing-aanval, waarbij iemand op een link in een e-mail heeft geklikt en zo de malware binnen laat. Iemand voert dan via een schijnbaar vertrouwde website zijn inloggegevens in en het hek is van de dam.

Tegenwoordig is malware-as-a-service in trek. Op 'ondergrondse' fora zijn setjes te koop. Een kind kan de was doen, bij wijze van spreken. Je hebt geen Hogeschool Informatietechnologie nodig om met deze malware aan de slag te gaan.

Actie: Leer alle betrokkenen riskante mails te herkennen en niet overal zomaar op te klikken. Gebruik antivirussoftware. Gebruik actuele software en pas patches zo snel mogelijk toe.

Voor een veilig beheer is het nodig ook inzicht te hebben in de koppelvlakken.

Falende infrastructuur: gebrek aan inzicht in de infrastructuur kan poorten openzetten waar kwaadwillenden dankbaar gebruik van maken. Dit is overigens niet beperkt tot de eigen omgeving. Steeds vaker zijn netwerken verknoopt met die van leveranciers, overheid, toezichthoudende instanties. En met de omgeving van cloud-dienstverleners. Voor een veilig beheer is het nodig ook inzicht te hebben in de koppelvlakken. Aanvallen verlopen immers ook steeds vaker via ketenpartners. Dus onderwijsinstellingen moeten de digitale relaties met hun leveranciers en andere ketenpartners onder de loep leggen.

Actie: Zorg voor goede, proactieve software voor beheer- en monitoring. Een algemene beveiligingsmaatregel is segmentering van de infrastructuur. Mocht één segment dan geïnfecteerd raken, dan kan dat segment worden afgesloten om te voorkomen dat de infectie zich verder verspreidt. Maak afspraken over hoe betrokkenen met hun endpoints (pc's, laptops, tablets, smartphones) moeten omgaan.

Uit het onderzoek van Kantar blijkt dat DDoS-aanvallen binnen het onderwijs het meest voorkomen, op de voet gevolgd door aanvallen met ransomware en malware. Dit heeft overigens in de meeste gevallen niet geleid tot verscherpte maatregelen om kwaadwillenden te weren. Er zijn nog tal van andere bedreigingen. Het voert te ver om daar op in te gaan. Wat wel gemeld dient te worden is dat een scherp oog nodig is om de steeds geraffineerdere aanvallen te herkennen. Hierbij wreekt zich het gebrek aan security-experts in de markt. Zelfs al is er talent aanwezig binnen de eigen IT-afdeling, dan nog gaan de ontwikkelingen zo snel dat het bijna ondoenlijk is om ze allemaal bij te houden, zeker als de persoon die dat zou moeten doen ook nog andere taken heeft dan de security op peil te brengen en te houden. De inzet van een managed security serviceprovider biedt dan uitkomst.

Een scherp oog is nodig om de steeds geraffineerdere aanvallen te herkennen.

De gevolgen

4

Cybercriminelen halen veel geld binnen (volgens Cybersecurity Ventures meer dan de totale winst die wordt gemaakt in de drugshandel) tegen bijzonder lage risico's. De kans dat ze worden gepakt en vervolgd, ligt in de VS op minder dan 1 procent. Het is aannemelijk dat dit percentage in Nederland niet veel anders is. Cybercrime, kortom, biedt aantrekkelijke mogelijkheden voor een lucratieve loopbaan. De verwachting is dan ook gerechtvaardigd dat de aanvallen zullen toenemen en steeds geraffineerder zullen worden. Cybersecurity Ventures schat dat tegen 2025 cybercrime wereldwijd 10,5 triljoen dollar kost.

Vier op de tien onderwijsinstellingen heeft te maken gehad met problemen op het gebied van IT-beveiliging.

Tijd- en energieverlies

Kantar interviewde onderwijsinstellingen over de gevolgen van cybercrime in het onderwijs. Tijd- en energieverlies worden genoemd als belangrijkste storend gevolg door 69%. Andere aspecten (in volgorde van meest genoemd) zijn verminderde bereikbaarheid, extra beveiligingskosten, verlies van continuïteit, herstelkosten, reputatieschade, verlies van gegevens, en losgeld. Dat de aanval geen gevolgen heeft gehad, wordt door 12% gezegd.

Een CIO geeft bij zijn antwoord de opmerking mee: "Onze onderwijsinstelling heeft sinds september 2019 met regelmaat last van DDoS-aanvallen. Gevolgen zijn dat verscheidene lessen beperkt tot geen doorgang kunnen vinden, dat administratief medewerkers web-diensten en allerlei applicaties niet kunnen gebruiken, enz. Kortom, extreem verstorende acties waar de hele organisatie last van heeft."

Directe en indirecte gevolgen

Geslaagde aanvallen hebben zowel directe als indirecte gevolgen. Onder de eerste categorie valt bijvoorbeeld het niet beschikbaar zijn van applicaties en gegevens voor studenten en personeel. Bij een DDoS-aanval is contact met de 'buitenwereld' miniem (heel soms kan er een bestand doorsijpelen). Dat betekent dat het onderwijs stil komt te liggen, maar bijvoorbeeld ook dat de boekhouding openstaande facturen niet kan betalen.

Bij een geslaagde ransomware-aanval is het directe gevolg het losgeld: de hoeveelheid geld die op tafel moet worden gelegd om de bestanden weer vrij te laten geven. Maastricht bijvoorbeeld betaalde 197.000 euro losgeld. Er zijn signalen dat de criminelen hun financiële eisen flink opschroeven, vanwege de eerder met hun ransomware geboekte successen.

Directe gevolgen van andere aanvallen kunnen zijn identiteitsfraude, diefstal van gevoelige informatie die vervolgens openbaar wordt gemaakt, financiële malversaties. In het Kantar-onderzoek meldt een CIO binnen het MBO: "Wijzigen bankrekeningnummer van medewerkers".

De indirecte gevolgen zijn ook niet mals. Stel dat een organisatie van de problemen afkomt zonder losgeld te hoeven betalen, dan nog is er veel geld nodig voor herstel en herinrichting van de systemen. Andere negatieve gevolgen zijn reputatieschade en de tijd van personeelskosten die nodig zijn om alles opnieuw en beter te organiseren. Als het onderwijs stil ligt, heeft dit gevolgen voor de slaagkansen van studenten. Het Staring College in het Gelderse Lochem en Borculo heeft losgeld betaald (het bestuur wil niet vertellen hoeveel) om examenleerlingen niet in de steek te laten. Bestuurder C.E. Krist-Spit zei tegen Omroep Gelderland:

> Deze situatie voelt voor alle betrokkenen als een nachtmerrie. Het besluit dat we hebben genomen gaat in tegen al onze principes, het voelt heel slecht. Echter, het belang om het onderwijs doorgang te laten vinden, juist in deze tijd, heeft de doorslag gegeven.

Tijdens het onderzoek bij het Staring College bleek dat ook de back-ups waren aangetast.

Stand van zaken

5

Hoe pakt het onderwijsveld op dit moment de uitdagingen op? Een verbijsterende 13 procent zegt helemaal niets op de agenda te hebben staan om de beveiliging te verbeteren. Het zou kunnen dat dit thema bij die 13 procent totaal niet speelt omdat alles prima op orde is. Maar gezien de resultaten van het door Kantar uitgevoerde onderzoek en het nieuws dat de dagbladen bereikt, valt dit te betwijfelen.

Bestuur en directie zeggen in 48 procent van de respondenten meer aandacht te willen besteden aan dit onderwerp. Onder meer door een intern communicatieplan op te stellen voor het omgaan met de cyber-risico's (37%), het inschakelen van externe expertise en tooling (33%) en het laten uitvoeren van een security scan door een expert (30%).

Als evenwel uit het onderzoek van Kantar blijkt dat 11% van het totale budget aan IT besteed wordt en dat binnen dit IT-budget bij het merendeel van de onderwijsinstellingen 5 tot 0% naar IT-security gaat, dan zien we hier een discrepantie tussen wens en werkelijkheid.

Drie uitspraken, gedaan in het onderzoek, tonen de twijfel over de ernst die directies en besturen aan de dag leggen:

"IT-medewerkers zijn flink met beveiliging bezig; zij willen het een plaats geven. Standaardzaken zijn over algemeen goed geregeld, maar het grootste probleem zit bij gebruikers. Alertheid op dingen die niet kloppen, is essentieel. Zolang het bestuur of de directie van de instelling deze ontwikkelingen (NB: daadwerkelijke problemen binnen de eigen instelling) niet als alarmerend ervaart, blijft het een lastig punt om op de agenda te houden."

"Een preventieve aanpak is van groot belang. Wie daar niet voor kiest, neemt bewust een aantal risico's. Het gaat nu allemaal goed en dat wil je zo houden, maar de ontwikkelingen gaan heel snel."

"Men heeft maar half in de gaten wat de impact is van identiteitsdiefstal. Het onderwijs grossiert in persoonsgegevens en digitalisering vraagt erom dat steeds meer systemen aan elkaar gekoppeld worden. Hoe groter de materie, hoe complexer het wordt (scholen worden ook groter) om een gedegen beveiliging op te zetten", meldt een IT-manager in het Kantar-onderzoek.

Deze onderschatting leidt ertoe dat de urgentie en het belang van passende IT-security niet de noodzakelijke aandacht krijgt. Ook hier laat het Kantar-onderzoek teleurstellende resultaten zien.

Vergelijk die 5% of minder van het IT-budget die aan privacy & security wordt besteedt met het bedrijfsleven, waar zo'n 26 - 29 % wordt besteed.

- Uit een onderzoek van security-specialist Kaspersky blijkt dat het aandeel van IT-security in het totale IT-budget binnen het MKB groeide van 23% in 2019 naar 26% in 2020. Voor grote ondernemingen was een groei te noteren van 26% in 2019 naar 29% in 2020. Voor onderwijs is dat niet inzichtelijk. Mogelijk omdat er binnen het onderwijs te weinig zicht is op uitgaven aan IT-security, óf omdat dat aandeel budgettair ernstig laag is. Maar in beide gevallen is duidelijk dat het belang van IT-beveiliging niet is doorgedrongen tot in de vezels van de besturen van onderwijsinstellingen.

In tegenstelling tot bijvoorbeeld de industrie of het bankwezen opereert het onderwijs in een tamelijk open omgeving. In het onderwijs is immers sprake een grotere diversiteit aan gebruikersgroepen: leerlingen/studenten, bestuur, docenten, ondersteunend personeel, leveranciers, toezichthoudende instanties. Elk van die groepen heeft zijn eigen gedrag, van normaal tot 'onderzoekend/experimenterend, terwijl de instelling het gebruik van IT ook weer laagdrempelig wenst te houden. Dit alles leidt tot een 'openheid' waarbij extra waakzaamheid nodig is.

Wat in het Kantar-onderzoek ook opvalt, is dat de pandemie bij slechts 33% van de onderwijsinstellingen heeft geleid tot aangescherpt IT-beveiligingsbeleid. Bij 63% is het beleid onveranderd. En bij een zeer kleine groep van 4 % is het beleid zelfs versoepeld. Tegelijkertijd is het aantal DDoS-aanvallen wereldwijd in 2020 met 80% toegenomen. Zulke aanvallen kunnen leiden tot een verstoring van het (online) lesproces. Het zou dus te verwachten zijn dat IT-beveiliging dan meer aandacht krijgt.

Het gevolg is dat in de media regelmatig melding moet worden gemaakt van geslaagde aanvallen op onderwijsinstellingen (zie binnenzijde cover). Vooral de geslaagde ransomware-aanval op Universiteit Maastricht eind 2019 heeft veel losgemaakt. De universiteit won de SURF Security en Privacy Award 2021 'voor de open wijze waarop het de kennis en ervaring deelde over de ransomware-aanval'. Zou het niet meer voor de hand hebben gelegen dat die prijs naar een onderwijsinstelling was gegaan die openlijk vertelt hoe je zo'n aanval kunt voorkomen?

Uit het feit, dat bij die aanval moest worden toegegeven aan afpersing, blijkt duidelijk dat onderwijsinstellingen niet beschikken over een disaster recovery plan, of DRP. In een dergelijk plan wordt stap voor stap aangegeven hoe te handelen bij een IT-calamiteit en wie in zo'n geval wat moet doen.

Leon van Lare, senior manager bij Stichting Onderwijs Midden-Limburg (SOML) en Manager ICT én Privacy Officer bij de onderwijsinstelling, formuleert het als volgt:

> Wij volgen de security norm ISO 27000; daar komt een disaster recovery plan niet in voor. Onze IT-dienstverlener IT-Workz, die momenteel een security scan bij ons uitvoert, heeft in een overleg aangegeven dat zo'n plan wel nodig is. Wij overwegen nu om dat op te stellen.

Dat een disaster recovery plan zinvol is, blijkt wel uit het aantal keren dat het mis is gegaan bij onderwijsinstellingen in Nederland.

Ontwikkelingen op het gebied van cyberveiligheid

Toch lijken er ook progressie te worden geboekt op het gebied van cyberveiligheid. De VO-Raad heeft begin maart SIVON en Google aangesproken op de privacyrisico's voor scholen die gebruikmaken van Google G Suite. Eind maart is de VO-raad samen met de PO-Raad, Kennisnet en SIVON van start gegaan met het Netwerk IBP (Informatiebeveiliging en Privacy). Dit netwerk is interessant voor iedereen die zich bij een onderwijsinstelling bezighoudt met beveiligings- en privacyvraagstukken: besturen uit het basis- en voortgezet onderwijs en functionarissen gegevensbescherming. De organisatie zit nog in de opstartfase.

Uit de Monitor IBP 2020 van de VO-raad, PO-Raad en Kennisnet blijkt dat er ten opzichte van het voorgaande jaar op alle onderdelen vooruitgang is geboekt. Er zijn ook nog aandachtspunten. In totaal hebben 3070 bestuurders van onderwijsinstellingen, schoolleiders, ict-coördinatoren, stafmedewerkers en docenten deelgenomen aan de Monitor IBP. Ongeveer de helft hiervan is werkzaam in het voortgezet onderwijs. Circa vier procent is werkzaam in het (voortgezet) speciaal onderwijs.

> Ondanks deze 'geconstateerde vooruitgang' weten criminelen de defensie bij onderwijsinstellingen nog steeds met succes te omzeilen.

Er moet, aldus de Monitor, meer aandacht komen voor bewustwording van iedereen binnen de onderwijsinstelling. Bijna 40 procent van de docenten geeft aan nog onvoldoende bewust gemaakt te worden van IBP. Die bewustwording zou bijvoorbeeld gestimuleerd kunnen worden door periodieke IBP-trainingen aan te bieden.

De Monitor laat ook zien dat privacy meer aandacht krijgt dan informatiebeveiliging. Het nemen van (technische) maatregelen is noodzakelijk om risico's rondom het gebruik van data te beperken. Denk aan het opstellen van procedures voor datalekken en het uitvoeren van Data Protection Impact Assesments (DPIA's). DPIA's zijn vaak arbeidsintensief en kostbaar, de VO-raad adviseert dan ook om dit samen met andere bestuurders van onderwijsinstellingen/scholen op te pakken.

Samenvattend is te stellen dat er binnen het onderwijsveld beweging is gekomen in de richting van betere IT-security, mede door Covid-19 en de gevolgen die de pandemie voor het onderwijs met zich meebrengt. Er is echter nog genoeg te doen om de cybercriminelen buiten de virtuele deur te houden.

Verantwoordelijkheid

6

De Algemene Verordening Gegevensbescherming (AVG) schrijft ook voor onderwijsinstellingen geldende regels voor met betrekking tot de verwerking van persoonsgegevens. Zo moeten onderwijsinstellingen bijvoorbeeld bijna altijd een Functionaris Gegevens Bescherming (Data Protection Officer) aanstellen. Hij [of zij] moet er onder andere op toezien dat de organisatie de AVG naleeft. Maar de eindverantwoordelijkheid ligt bij de onderwijsinstelling. En die verantwoordelijkheid heeft betrekking op de organisatorische én technische inrichting.

Bij technische inrichting valt te denken aan:

- logische en fysieke (toegangs-)beveiliging en beveiliging van apparatuur (denk niet alleen aan kluizen en portiers, maar ook aan firewalls en netwerksegregatie);
- technisch beheer van de (zo beperkt mogelijke) autorisaties en bijhouden van logbestanden; beheer van technische kwetsbaarheden (patch management);
- software actueel houden;
- back-ups maken;
- automatisch verwijderen van verouderde gegevens;
- versleuteling van gegevens;
- hashing (pseudonimiseren van persoonsgegevens).

> Het bestuur moet zorgen voor een veilige omgeving, zowel technisch als organisatorisch. Dus ervoor zorgen dat betrokkenen weten hoe je veilig met informatie kunt omgaan.

Geen jurisprudentie

Volgens Arnoud Engelfriet, partner bij ICTRecht, en Nienke Bernard, advocaat bij Greenberg Traurig, is het in het geval van de AVG tamelijk goed geregeld waar de verantwoordelijkheid ligt. “Dat is het bestuur van de onderwijsinstelling. Tenzij duidelijk in een overeenkomst is vastgelegd dat de verantwoordelijkheid berust bij de directeur of directie.” Zijn collega is het hier niet helemaal mee eens; zij meent dat te allen tijde het bestuur verantwoordelijk is. Overigens is er nog geen jurisprudentie op dit vlak.

De verantwoordelijkheid voor de data in het geval van diefstal of beschadiging, ligt ook het bestuur. Wat gebeurt er bijvoorbeeld als een ransomware-aanval succesvol is omdat een student per ongeluk op een kwaadaardige link heeft geklikt in zijn e-mail? Is die student dan verantwoordelijk? “Nee”, aldus Engelfriet, “Het bestuur moet zorgen voor een veilige omgeving; zowel technisch als organisatorisch. Dus ervoor zorgen dat betrokkenen weten hoe je veilig met informatie kunt omgaan.”

Beiden wijzen erop dat de bestuurders van onderwijsinstellingen maatregelen moeten nemen om IT-Security daadwerkelijk te waarborgen. De overheid moet dit actief stimuleren en nastreven, bijvoorbeeld door een gedragscode voor IT-beveiliging op te stellen, en ervoor te zorgen dat die wordt nageleefd.

"Er bestaan gedragscodes in andere branches, maar er is nog geen uniforme code voor het onderwijs. Er is ook nog geen proces ingericht voor het goedkeuren van die code. Partijen als Accenture en KPMG staan te popelen om hiermee aan de slag te gaan. Overigens zou de VO-Raad dit ook kunnen oppakken. Ik schat dat het nog wel een paar jaar duurt voordat er zo'n code is," licht Engelfriet toe.

Er is echter een verschil tussen verantwoordelijkheid en aansprakelijkheid.

"Wil een bestuurder persoonlijk aansprakelijk worden gesteld voor geleden schade als gevolg van bijvoorbeeld een ransomware-aanval, dan moet hij of zij het wel heel bont hebben gemaakt; ik zie dat niet snel gebeuren", stelt Bernard. Zij geeft overigens aan dat criminelen het onderwijs als een snoepwinkel zien. "Geen wonder als je nagaat hoeveel en welke data daar zijn opgeslagen. Daarom is het belangrijk dat onderwijsinstellingen goed in kaart brengen welke risico's zij lopen."

Verzekeraars stellen eisen

Engelfriet geeft aan dat ook verzekeraars zich op dit terrein roeren. "Zij zullen eisen stellen. Bijvoorbeeld dat de IT moet voldoen aan geldende ISO-normen, dat awareness-trainingen aantoonbaar worden gehouden, dat er offline back-ups zijn. Als niet aan die eisen is voldaan, zullen zij niet uitkeren in geval van opgetreden schade. Dus ook niet waar het gaat om het geld dat nodig is om de systemen te herstellen na een geslaagde aanval. Verzekeraars zullen eisen dat accountants in hun jaarverslagen dit aspect aan bod laten komen." De vraag is overigens, nuanceert hij, of besturen van onderwijsinstellingen wel weten dat je je kunt verzekeren tegen cybercriminaliteit.

Meer regelgeving vinden beiden niet nodig. "Er is al genoeg en je moet niet alles willen juridiseren. Het is ook een politieke kwestie om ervoor te zorgen dat het onderwijs zijn IT-beveiliging op orde heeft en daar ook budget voor beschikbaar stelt. Het kan immers niet zo zijn dat ongenode gasten het curriculum van een onderwijsinstelling kunnen veranderen of cijferlijsten gaan aanpassen, waardoor diploma's geen waarde hebben. De bestuurders zijn hiervoor verantwoordelijk, de overheid moet zorgen dat zij die verantwoordelijkheid nemen én kunnen uitvoeren", licht Engelfriet toe.

Discrepantie in verantwoordelijkheidsbesef

Het tweetal vindt, gezien de vele keren dat het mis gaat, dat bestuurders van onderwijsinstellingen, in tegenstelling tot bijvoorbeeld de financiële sector, zich niet bewust zijn van de urgentie om hun IT-beveiliging op orde te brengen. “Het kan zijn dat de overheid stappen gaat nemen en bijvoorbeeld gaat korten op subsidie als een onderwijsinstelling het niet goed voor elkaar heeft,” verwacht Bernard.

Dat de bestuurders van onderwijsinstellingen verantwoordelijk zijn, is niet bij iedereen bekend. Uit het Kantar-onderzoek blijkt dat de meerderheid van onderwijsbestuurders vindt dat het aan de onderwijsinstellingen is om verantwoordelijkheid te nemen. Tegelijkertijd blijkt echter dat een (groot) deel van de onderwijsbestuurders niet door heeft dat ze als bestuurder, zelfstandig en persoonlijk, feitelijk verantwoordelijk zijn. Op de vraag wie eindverantwoordelijk is voor IT-beveiliging binnen de onderwijsinstelling wijst 77% naar de directie dan wel de voorzitter van de Raad van Bestuur. In de praktijk wordt echter bij twee op de drie onderwijsinstellingen slechts 5 % of minder van het IT-budget toegewezen aan IT -beveiliging; er is dus sprake van een discrepantie tussen intentie en daadwerkelijk gedrag.

Wat kan de overheid doen?

7

Wie de partijprogramma's voor de Tweede Kamerverkiezingen in maart 2021 bestudeert, moet vaststellen dat – hoewel de meeste programma's wel ingaan op IT-veiligheid en cybercriminaliteit –nergens specifiek aandacht wordt besteed aan het belang van IT-security voor het onderwijs. Ook niet waar andere cyberveiligheidsdomeinen of vitale sectoren wél specifiek uitgelicht werden.

Het jaar 2020 kenmerkte zich door onderwijs op afstand als gevolg van de COVID-19 pandemie. Daarbij stellen onderwijsinstellingen zich voor videoconferencing en online proctoring afhankelijk op van enkele cloud-dienstleveranciers buiten de Europese Economische Regio: Amazon, Google, ZOOM en Microsoft.

Cyberveiligheid en informatie-veiligheid zijn in deze snel digitaliserende wereld belangrijker dan ooit.

Dé relevant vraag daarbij is: waar worden de data van de ("onze") studenten en docenten opgeslagen? Voldoende, transparant zicht daarop ontbreekt bij een deel van de aanbieders van data services. Het is een wezenlijke uitdaging: het ongeldig verklaren van Privacy Shield door het Europese Hof van Justitie zou, bij ongewijzigd beleid, uiteindelijk kunnen leiden tot continuïteits-problemen doordat de regels ten aanzien van gegevensopslag zoals gehanteerd door de Europese- en Nederlandse overheid afwijken van de regels die door bepaalde cloud-dienstleveranciers worden voorgeschreven. De overheid kan en moet dus gaan nadenken over duidelijke regelgeving ten aanzien van (en daarmee ook toezicht op) de locaties waar data opgeslagen zouden moeten worden, binnen wet- en regelgeving.

Wat zou de overheid kunnen doen om de IT-beveiliging bij onderwijsinstellingen naar een hoger plan te tillen? Hierbij is het nuttig met een schuin oog te kijken naar wat het Rijk doet op het vlak van duurzaamheid: er wordt een bij aanbestedingen bijvoorbeeld een duurzaamheids-paragraaf geëist en de aangedragen duurzaamheidsoplossingen leveren een specifieke (hogere) score. Provinciale overheden doen hetzelfde om duurzaamheid en circulariteit te stimuleren.

Ontwikkel een raamwerk

Naar analogie van die benadering zou het Rijk van bestuurders van onderwijsinstellingen kunnen eisen dat zij in hun jaarverslagen beschrijven welke maatregelen ze hebben genomen om een cyberveilige omgeving te creëren. Aan de hand van een door het Rijk te ontwikkelen raamwerk dat aangeeft waar een cyberveilige onderwijsinstelling aan móet voldoen en welke variabele factoren daar bovenop tot een extra score leiden, kan de door een onderwijsinstelling gerealiseerd niveau van beveiliging meewegen in het budget dat een onderwijsinstelling van het Rijk ontvangt. Dat raamwerk zou het Rijk moeten opstellen in nauwe samenspraak met het onderwijsveld en het bedrijfsleven (de securityspecialisten en -dienstverleners). De uitvoering daarvan zou in handen gelegd kunnen worden van onafhankelijke accountants, de VO-raad, MBO-raad of (in het geval van hoger onderwijs) SURF. De toetsing van de geïmplementeerde maatregelen aan dat raamwerk zou vervolgens onafhankelijk belegd moeten worden, bij de controlerend accountant. Door hier tevens, transparant, in het jaarverslag over te rapporteren ontstaat ook vertrouwen. Op deze wijze voldoen onderwijsinstellingen ook aan de door hen zelf opgelegde Good Governance code.

De verantwoordelijkheid voor cybersecurity zou expliciet moet worden gelegd bij het bestuur van de onderwijsinstelling. Zij is immers ook verantwoordelijk en aansprakelijk. De verantwoordelijkheid kan niet belegd worden bij de IT-afdeling, die over onvoldoende middelen beschikt.

Bewustwording

8

In IT-kringen praat men steeds over awareness. Wat daarmee in die context wordt bedoeld, is dat mensen zich bewust zijn van de risico's bij het gebruik van computers die verbonden zijn met (openbare) netwerken. Voor IT'ers is het altijd schipperen tussen maximale beveiliging en gebruiksgemak. Je kunt alles dichtgooien, dan weet je zeker dat er geen ongenode gasten binnenkomen. Maar tegelijkertijd valt er dan niet meer te werken. Het is zaak de gulden middenweg te vinden. Met het besef dat elke keten zo sterk is als de zwakste schakel. In dit geval: de mens. Daarom moet de aandacht gericht zijn op het instrueren van gebruikers: awareness-trainingen in jargon. Van alle datalekken wordt 95% veroorzaakt door menselijk handelen (Cybint). Volgens Cybint ligt de oorzaak vrijwel nooit bij de IT-afdeling zelf.

Bestuur en directieleden praten alleen over docenten en ondersteunend personeel als ze het over bewustwording hebben.

Nauwelijks awareness

Uit het onderzoek dat Kantar heeft uitgevoerd, blijkt dat de IT-afdelingen ontevreden zijn met de aandacht die besturen van onderwijsinstellingen hebben voor dit onderwerp: te weinig, nauwelijks budget voor. Slechts af en toe vinden trainingen plaats. Nieuwe medewerkers krijgen wel enige uitleg, maar het is niet iets dat vaak wordt herhaald, ook al zou dat moeten. Besturen en directieleden praten overigens alleen over docenten en ondersteunend personeel als ze het over bewustwording hebben; voor studenten bestaan geen programma's. Het bestuur gaat ervan uit dat dit onderwerp ter sprake komt tijdens lessen over informatietechnologie. Er lijkt vrijwel nergens een gericht programma om awareness uit te dragen. Zo zal dit onderwerp niet aan bod komen tijdens functioneringsgesprekken, waarbij dat niet eens bedoeld zou moeten zijn om ze een 'awareness-cijfer' te geven (want dat is bijna ondoenlijk), maar gewoon om het belang ervan te onderstrepen.

Veiligheid als cultuur

Laten we een uitstapje maken naar de petrochemische industrie. Als daar iets fout gaat, kan de boel ontploffen en staan er mensenlevens op het spel. Alle medewerkers krijgen voortdurend trainingen om veilig te werken. In de fabriekshal hangt een schema dat aangeeft hoeveel dagen het bedrijf ongevalsvrij is. Aannemers en onderaannemers die op het terrein aan de slag moeten, kunnen pas hun werk doen nadat zij uitvoerig zijn voorgelicht over de risico's die zij (en het bedrijf) lopen en hoe die zijn te vermijden. Bezoekers komen pas voorbij de portier nadat zij een filmpje hebben bekeken over de veiligheidsvoorschriften die ter plekke gelden.

Dit betekent niet dat er nooit iets fout kan gaan. Honderd procent garanties bestaan niet op dit vlak. Maar het creëert wel een sfeer van samen ervoor zorgen dat het niet mis kan gaan. Mensen zijn zich nadrukkelijk bewust van de risico's en hoe ze daarmee moeten omgaan. En dan wordt dat ook nog eens van tijd tot tijd gecontroleerd door de Arbeidsinspectie.

Continu proces

Goed, binnen het onderwijs zullen er geen doden vallen als een systeem wordt gehackt. Niettemin bestaan er grote risico's. Er gaan dan ook stemmen op om bewustwording van overheidswege verplicht te stellen en dus ook te controleren op naleving van de regels. Die mening hoor je overigens in IT-kringen, niet bij bestuurders van onderwijsinstellingen.

Creëer bewustwording

Hoe regel je awareness? Hoe zorg je ervoor dat binnen de organisatie een cultuur van 'veilig computeren', van een 'security-onderbewustzijn' ontstaat? Allereerst: dit is geen project, maar een (continu) proces. Daarbij kan gedacht worden aan de volgende stappen:

- **Het begint inderdaad met een cultuurverandering**, waarbij je moet beseffen dat elke verandering weerstand oproept. Leg daarom de regels niet alleen maar op, maar leg ze vooral uit. Verklaar het belang van een goed security-beleid. Cultuurverandering moet worden gedragen door het management; directie en bestuur moeten het voorbeeld geven.

- **Bepaal hoe het ervoor staat met het veiligheidsbewustzijn.** Bijvoorbeeld door te meten hoeveel incidenten worden gerapporteerd en om wat voor incidenten het gaat. Kijk bijvoorbeeld eens hoelang het duurt voordat iemand een rondslingerende usb-stick in de pc of laptop plaatst.

- **Leg vervolgens vast welk niveau** van veiligheidsbewustzijn nodig is. En bepaal een strategie om het verschil tussen bestaande en gewenste situatie te overbruggen. Kies slimme momenten om het onderwerp onder de aandacht te brengen, bijvoorbeeld bij indiensttreding, bij upgrades van een systeem, bij migratie naar of fusie met een andere onderwijsinstelling.

- **Gebruik digitale awareness-trainingen.** Bijvoorbeeld een programma dat een bericht laat zien als 'weet u zeker dat u naar deze site wilt?' als een vreemde URL wordt aangeklikt. Iets dergelijks kan ook met e-mail. Monitor welke mensen meedoen aan deze trainingen en maak dit bespreekbaar. Overweeg beloningen voor positief gedrag en maak veiligheidsbewustzijn onderdeel van beoordelingen.

- **Neem contact op** met een serviceprovider die hiermee ervaring heeft.

Te ondernemen stappen

9

Het is belangrijk dat er een goede beveiligingscultuur binnen de organisatie leeft én dat alles in het werk wordt gesteld dat technisch en organisatorisch mogelijk is om criminelen de loef af te steken. Hoe doe je dat?

- **Creëer bewustwording op twee niveaus.** Allereerst moeten bestuurders van onderwijsinstellingen zich bewust zijn van hun verantwoordelijkheid aangaande bescherming van data. Het tweede niveau is dat alle betrokkenen zich bewust moeten zijn van de risico's die het gebruik van computers met zich meebrengt. Hier komen awareness-trainingen in beeld. Maak hier serieus werk van. Dat betekent onder meer dat de trainingen consequent moeten worden aangeboden, dat gecontroleerd wordt wie ze gebruikt en dat dit onderwerp van gesprek is tijdens functioneringsgesprekken.

- **Controleer of alle hardware én software actueel is.** Dat wil zeggen: ga na of hardware beschikt over de nieuwste firmware en controleer of software in de nieuwste versie wordt gebruikt. Stel een patch-protocol op: zo snel mogelijk updates doorvoeren en testen.

- **Ga na of er geen schaduw-IT wordt toegepast.** Denk aan medewerkers die (buiten de IT-afdeling om) een SaaS-toepassing gebruiken. Pas als centraal inzichtelijk is welke programmatuur en diensten worden gebruikt, is het mogelijk dit goed te beheren. Het is overigens verstandig om een IT-dienstverlener met kennis en vaardigheden op het vlak van IT-Inrichting, -beheer en -security in de arm te nemen. Dit levert nieuwe inzichten.

- **Laat periodiek nagaan** of alle systemen nog voldoen aan de gestelde eisen. Het gebruik van informatietechnologie is voortdurend aan verandering onderhevig. Daarom moet van tijd tot tijd worden nagegaan of alles nog klopt. Zorg bovendien dat hiervoor geld in de begroting wordt gereserveerd.

- **Zorg dat de organisatie voldoet** aan de wereldwijd gehanteerde Critical Security Controls for Effective Cyber Defense van het Center for Internet Security; ook bekend als de CIS controls. Dit omvat een lijst met 20 maatregelen, verdeeld over basic, foundational en organizational. Wie deze basishygiëne op orde heeft, voorkomt de meeste cyber-ellende.

- **Zorg voor voldoende middelen** om een juist databeschermingsbeleid in te voeren en toe te passen. Uit het Kantar-onderzoek blijkt dat binnen het onderwijs door door een groot gedeelte van de onderwijsinstellingen slechts 5% of minder van het totale IT-budget wordt besteed aan security. Dit is ten enenmale onvoldoende. In andere sectoren ligt het gemiddelde rond de 25%. Ga hierover als onderwijsbestuurder het gesprek aan met de overheid.

- **Laat een deskundige partij zo snel mogelijk een security scan uitvoeren.** De Onderwijs ICT Securityscan is specifiek gericht op leerinstellingen. Toepassing ervan brengt alle kwetsbaarheden aan het licht en legt de bevindingen vast in een uitvoerig rapport. Onder andere de Katholieke Scholengemeenschap Etten-Leur heeft zo'n scan laten uitvoeren. Conrector Bedrijfsvoering Leon Geers: "We kregen een indrukwekkend rapport van 59 pagina's en in een presentatie werden direct de highlights doorgenomen. Het rapport zat zo in elkaar dat er voor onderdelen steeds op een schaal van één tot vier werd aangegeven hoe we scoorden. Waarbij een vier ongeveer een Fort Knox is qua veiligheid. Daarbij was het wel prettig dat er rekening werd gehouden met onze context. We zijn immers geen bank, maar een onderwijsorganisatie. Een twee kan in sommige gevallen juist best voldoende zijn."

- **Stel een Disaster Recovery Plan** (DRP) vast. Een dergelijk plan beschrijft welke stappen nodig zijn om na een calamiteit (bijvoorbeeld een brand of een menselijke fout) alle systemen weer als vanouds werkend te krijgen. Een DRP is onderdeel van de bedrijfscontinuïteitsplanning en raakt alle aspecten van een organisatie die afhankelijk zijn van een functionerende IT-infrastructuur. Overigens is het van belang om een DRP regelmatig in de praktijk te testen. Dit draagt bij aan een cultuur van IT-security en legt bovendien bloot of aanpassingen nodig zijn. Een goed noodherstelplan moet betrekking hebben op een breed scala aan potentiële incidenten. Voorbeelden zijn hardwarestoringen, natuurrampen, cybercriminaliteit en menselijke fouten.

- **IT-beveiliging is niet iets dat 'je er even bij doet'.** Er is brede én diepgaande kennis voor nodig die voortdurend moet worden bijgeschaafd, omdat de ontwikkelingen op dit vlak erg snel gaan. Dergelijke experts zijn schaars. Daarom verdient het aanbeveling op zoek te gaan naar een managed serviceprovider die ook security in zijn portfolio heeft. Je kunt ervoor kiezen al het dataverkeer te laten verlopen via de systemen van de managed security serviceprovider. Let wel: het bestuur blijft te allen tijde verantwoordelijk voor correct beheer van de data.

De te ondernemen stappen op (technisch) vlak zijn in het kort:

- Neem de bestaande strategie voor databeveiliging onder de loep. Zorg dat je real-time inzicht krijgt en data geautomatiseerd kunt herstellen.
- Organiseer de back-up volgens de 3-2-1-aanpak: minimaal drie kopieën, op twee afzonderlijke locaties waarvan minstens één buiten het pand.
- Oefen het disaster recovery plan minstens eens per maand. Het data- en applicatielandschap verandert voortdurend, dus voorkom dat je plan niet meer voldoet.
- Voer security patches en security updates zo snel mogelijk door.
- Versleutel je data. Encryptie van het netwerkverkeer voorkomt dat onbevoegden met je data aan de haal gaan.
- Gebruik opslagtechnologie waarmee het onmogelijk wordt om data aan te passen of te verwijderen. Dit voorkomt dat ransomware je back-up versleutelt of zoek maakt.
- Hanteer access management, waarbij de toegang van medewerkers afhankelijk is van hun rol, functie en daarbij behorende rechten, en het tijdstip waarop zij gerechtigd zijn van het systeem gebruik te maken. Gebruik hierbij multifactor authenticatie; alleen gebruikersnaam en wachtwoord is niet afdoende.
- Segmenteer het netwerk; als één onderdeel is geïnfecteerd, kun je dit afsluiten zonder gevolgen voor de rest van het systeem (en de bedrijfsvoering).

Colofon

Over Breens Network

Dit rapport is een uitgave van Breens Network. Wij zijn een Nederlandse ICT-organisatie, die al meer dan 25 jaar haar klanten ondersteunt bij hun digitale transformatie om zo de effectiviteit, kwaliteit van de output, (kosten) efficiëntie en flexibiliteit van hun organisaties te vergroten.

Met merken Educator, IT-Workz, MBOwebshop, SLBdiensten en Slim.nl bedient Breens Network onderwijsinstellingen in het vo, mbo en ho. We zijn ook actief in de zorg en werken voor decentrale overheden. In totaal maken meer dan 1 miljoen leerlingen en studenten, 90.000 docenten en 40.000 medewerkers gebruik van onze diensten.

Dit rapport is een samenwerking van Breens Network met Teus Molenaar en is mede gebaseerd op de uitkomsten van het onderzoek dat door Kantar is uitgevoerd (zie hierna). Teus werkt sinds 1992 als ICT-journalist. Schrijft onder andere voor Dutch IT Channel en Computable veel over IT-security.

'Lerend Nederland' is gefotografeerd door Ruby Cruden. Sinds 2016 analoog en digitale fotografe. Nieuw Nederlands Talent, een ambitieuze fotografe, filmmaker en experimenteel schrijfster.

Meer weten? Kijk op www.breensnetwork.nl. Of neem contact met ons op via 088 489 6900 of via info@breensnetwork.nl.

Breens Network
Fred. Roeskestraat 115
1076 EE Amsterdam

Disclaimer

Breens Network heeft de grootst mogelijke zorgvuldigheid betracht bij het samenstellen van dit rapport. Echter voor onjuistheden en onvolledigheden met betrekking tot de inhoud vanhet rapport, op welke grond dan ook, kunnen Breens Network en/of de samenstellers daarvan op geen enkele wijze verantwoordelijk worden gesteld. Geen enkele aansprakelijkheid wordt aanvaard.

Bronnenlijst (gerangschikt op nummer en van boven naar beneden in de tekst)

1.1 Computable https://www.computable.nl/artikel/opinie/security/7092654/1509029/onderwijsinstellingen-stevenen-af-op-cyberramp.html
1.2 Global Competitiveness Report https://www.weforum.org/reports/the-global-competitiveness-report-2020
1.3 University of Maryland https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds
2.1 Verizon data breach report 2020 https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
2.2 Microsoft tracker https://www.microsoft.com/en-us/wdsi/threats
2.3 en 3.1 Sophos https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
3.2 en 5.1 Kaspersky https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_IT%20Security%20Economics%202020_Executive%20Summary.pdf
3.3 NBIP https://www.nbip.nl/wp-content/uploads/2021/04/NBIP-Rapport-DDoS-data-2020.pdf
4.1 https://www.omroepgelderland.nl/nieuws/6770476/Staring-College-betaalt-losgeld-na-grote-cyberaanval
5.2 VO-raad https://www.vo-raad.nl/nieuws/surf-en-sivon-spreken-google-aan-op-privacyrisico-s
8.1 Cybint https://www.cybintsolutions.com/cyber-security-facts-stats/
9.1 https://www.cisecurity.org/controls/cis-controls-list/
9.2 https://www.onderwijsictsecurityscan.nl/

Bronnen overzicht: waar ging het mis

1. Veilig internetten https://d15k2d11r6t6rl.cloudfront.net/public/users/Integrators/a0a42ab5-3cb9-4912-84b7-3c6e47330d5c/smart-pr-805/HvdM%20Hacken%20oktober%202018%20rapport_3.pdf
2. NRC https://www.nrc.nl/nieuws/2021/02/26/gelderse-school-betaalt-losgeld-vanwege-hack-maandag-geen-les-a4033498
3. Volkskrant https://www.volkskrant.nl/nieuws-achtergrond/wetenschapsfinancier-nwo-gehackt-en-afgeperst-door-bekende-ransomwaregroep~bc78948f/
4. UVA https://services.uva.nl/
5. Parool https://www.parool.nl/amsterdam/hackers-roven-persoonlijke-gegevens-studenten-inholland~b4a4f2c5/?referrer=https%3A%2F%2Fwww.google.com%2F
6. RTL https://www.rtlnieuws.nl/tech/artikel/5011241/universiteit-maastricht-betaalde-losgeld-hackers
7. Computable https://www.computable.nl/artikel/nieuws/overheid/7126602/250449/heropbouw-ict-hof-van-twente-na-hack-vergt-25-jaar.html
8. Trouw https://www.trouw.nl/binnenland/hackers-stelen-privegegevens-afgestudeerden-tu-delft-en-uu~b871380d/?referrer=https%3A%2F%2Fwww.google.com%2F
9. AD https://www.ad.nl/zoetermeer/porno-in-beeld-tijdens-digitale-les-op-erasmus-college-lerares-in-tranen~accdc7d2/?referrer=https%3A%2F%2Fwww.google.com%2F
10. De Limburger & 1Limburg https://www.limburger.nl/cnt/dmf20200220_00148455
https://www.1limburg.nl/ruim-20-limburgse-scholen-getroffen-door-computervirus?context=latestarticles
11. Omroep Zeeland https://www.omroepzeeland.nlnieuws/125865/Zeeuws-Vlaamse-scholen-doelwit-van-reeks-ddos-aanvallen
12. AD https://www.ad.nl/tech/universiteit-vijf-keer-doelwit-ddos-aanval-tentamen-afgelast~a6853703/

IT-beveiliging binnen het voortgezet- en middelbaar beroepsonderwijs

breens network

KANTAR

Inhoudsopgave

Samenvatting

In December 2020 heeft Breens Network, KANTAR verzocht om een onderzoek uit te voeren naar de 'staat van Privacy & Security' in het voortgezet en middelbaarberoepsonderwijs. Een en ander ter onderbouwing van de visie van Breens Network dat Privacy & Security voorwaardelijk is voor een optimale leer/werk omgeving van leerlingen, studenten, docenten en medewerkers van schoolinstellingen. Alleen al vanwege het kunnen garanderen van een veilige omgeving zou het hoog op de agenda moeten staan van bestuur en directie.
Alle informatie is gebaseerd op resultaten vanuit een online enquête die door KANTAR is ingezet in opdracht van Breens (27-1-2021 t/m 12-02-2021). Hierin zijn bestuurs-, directieleden, CIO's en IT-medewerkers binnen het VO en MBO opgenomen. In totaal hebben er 115 personen deelgenomen aan dit onderzoek. In de bijlage is de door KANTAR gebruikte onderzoeksopzet vermeld.

- IT beveiliging staat na het waarborgen van kwaliteit van het onderwijs hoog op de agenda van bestuur, directie en IT medewerkers .Daarentegen is een kwart van het voortgezet onderwijs én MBO instellingen (zeer) kwetsbaar voor aanvallen. Acties rondom IT beveiliging lijken vaak reactief van aard, men onderneemt stappen zodra een aanval heeft plaatsgevonden.

- De onbekendheid met de aantrekkelijkheid van het onderwijs voor cybercrimaliteit is alarmerend groot. Men is op de hoogte van de grootte van het probleem maar heeft niet in de gaten dat dit zich grotendeels binnen de eigen sector afspeelt.

- De omvang van het probleem neemt ondertussen alleen maar toe door vergaande digitalisering van het onderwijs. Daar bovenop komen externe ontwikkelingen zoals explosief toenemende hacks gericht op het ontvreemden van persoonsgegevens; welke in grote getalen aanwezig zijn binnen het onderwijs.
De manier van lesgeven is volledig op zijn kop gegooid door Corona en is meer dan ooit afhankelijk van IT. DDos aanvallen kwamen al het meest voor binnen de sector maar de pandemie heeft voor een stijging gezorgd. Ondanks deze situatie ziet slechts 1 op de 3 onderwijsinstellingen de noodzaak tot aanscherpen van IT beveiliging.

- 4 op de 10 instellingen hebben het afgelopen jaar te maken gehad met daadwerkelijke aanvallen die veel tijd, energie en geld hebben gekost. Het gaat vaak om het platleggen van de systemen, ongeautoriseerde toegang tot systemen en het lekken van persoonsgegevens. Het bestuur en directieleden zijn hiervoor verantwoordelijk. Zelf is men het hier mee eens, IT medewerkers zien echter niet altijd terug dat het juiste belang gehecht wordt aan IT beveiliging. De meerderheid geeft slechts 5% of minder van het IT-budget uit aan beveiliging.

- Het beeld dat geschetst wordt voor de toekomst is redelijk goed. Een deel van de onderwijsinstellingen heeft acties op de planning staan én is bereid om (meer) te investeren. De aanpak is voornamelijk gericht op coaching van medewerkers en over het algemeen meer aandacht voor IT beveiliging; vraag blijft of hier de juiste focus op het juiste moment voor is. De wisselwerking tussen intentie en gedrag is van groot belang Hoe kan men ervoor zorgen dat goede intenties ook leiden tot daadwerkelijk gedrag. Niet alleen als reactie op een aanval maar écht als proactief gedrag om de IT beveiliging te verbeteren en risico's te voorkomen.

DE NOODZAAK VAN IT-BEVEILIGING WORDT ONDERSCHAT

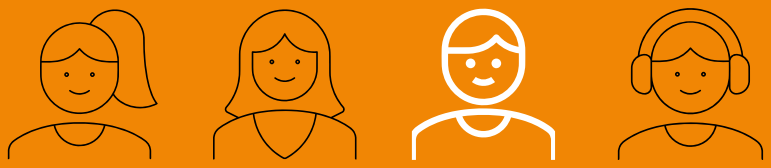
Dreigings-niveau is herken-baar maar wordt niet gelinkt aan de onderwijssector

500.000 aanvallen per maand, voornamelijk gericht op het onderwijs

81% weet niet dat dit probleem vooral speelt binnen het onderwijs

FINANCIËN STAAN OVER HET ALGEMEEN ONDER DRUK

Onderwerp staat op de agenda maar krijgt slechts zeer beperkt budget toegewezen



Een kwart van de instellingen is
(zeer) kwetsbaar

IT-MEDEWERKERS MISSEN VAAK EEN PROACTIEVE HOUDING BIJ BESTUUR

Beleid nauwelijks aangescherpt (1:3) ondanks toegenomen kwetsbaarheid in pandemie

Vaak voorkomende gevolgen:

- Platleggen van infrastructuur; continuïteit van het onderwijs komt in gevaar
- Ongeautoriseerde toegang tot data én systemen; lekken van persoonsgegevens

Bereidheid tot verbetering in zicht; bestuur / directie is eind-verantwoordelijk

Items op de agenda van 2021:

45% coaching

41% meer aandacht voor IT-beveiliging

37% intern commu-nicatieplan (bewustwording)

Alle informatie is gebaseerd op resultaten vanuit een online enquête die door Kantar is ingezet in opdracht van Breens (27-1-2021 t/m 12-02-2021). Hierin zijn bestuurs-, directieleden, CIO's en IT-medewerkers binnen het VO en MBO opgenomen. In totaal hebben er 115 personen deelgenomen aan dit onderzoek.

IT-beveiliging staat op de agenda maar externe ontwikkelingen zorgen voor een toenemend belang waar men zich slechts deels bewust van is. Een kwart van de scholen loopt (nog) een groot risico.

1

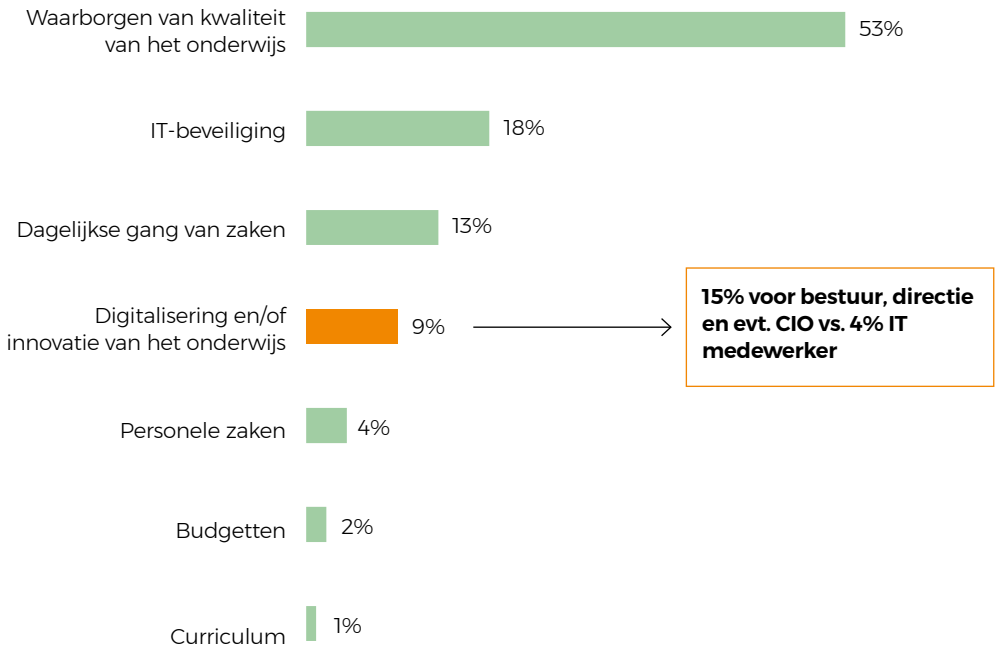
Digitalisering én IT beveiliging spelen na het waarborgen van de kwaliteit van het onderwijs belangrijke rol op de agenda van bestuurders én IT medewerkers binnen het VO en MBO

Het eerste punt staat met name hoog op het prioriteitenlijstje van de bestuurders, de directie en een eventuele CIO. Beiden zijn een belangrijke factor om het grootste belang, kwaliteit van onderwijs, te (blijven) borgen.

Toelichting vanuit IT experts:
"Beveiliging wordt steeds belangrijker, IT was altijd al belangrijk. Het onderwijs digitaliseert."

"Het IT gebruik neemt toe, er is steeds meer digitaal beschikbaar. Er dient een zekere mate van awareness bij de medewerkers te liggen maar ook de organisatie moet een bepaalde mate van volwassenheid hebben. Het bestuur moet belang hechten aan IT en op de hoogte zijn van de noodzaak tot gedegen beveiliging.

Kunt u de onderwerpen rangschikken op basis van belang binnen uw onderwijs-instelling ? (n=99)



Basis bestuur, directie, CIO = 41, IT medewerker = 49. Beiden indicatief n<50.

De noodzaak tot waarborgen van kwaliteit én de toenemende digitalisering van het onderwijs maakt nog niet dat het onderwijs de juiste actie neemt om risico's van IT gebruik te beheersen

Gemiddeld **3420*** leerlingen of studenten per instelling waarvan de gegevens mogelijk op straat komen te liggen én waarvoor de continuïteit van goed onderwijs gevaar loopt.

De overige 38% is minder uitgesproken en kiest voor een neutrale positie. Men sluit enige vorm van kwetsbaarheid niet uit. Hiermee komt wederom een groot risico voor het onderwijs en haar leerlingen / medewerkers in beeld.

Slechts 2 van de 5 onderwijsinstellingen geeft aan niet kwetsbaar te zijn voor problemen met IT beveiliging.

(Zeer) kwetsbaar gebruik

Neutraal

Niet of nauwelijks kwetsbaar

1 op de 4 scholen is (zeer) kwetsbaar voor problemen met IT-beveiliging

* Hoeveel leerlingen / studenten telt de onderwijsinstelling waarvoor u werkzaam bent? Indien de onderwijsinstelling waarvoor u werkt meerdere vestigingen heeft zijn wij op zoek naar het aantal leerlingen / studenten voor de totale organisatie. (n= 91)
Hoe kwetsbaar denkt u dat de onderwijsinstelling waar u werkt is? (n=115)

Als het kalf verdronken is dempt men de put; het inzetten van IT-beveiliging binnen het onderwijs is vaak reactief én tevens onvoldoende

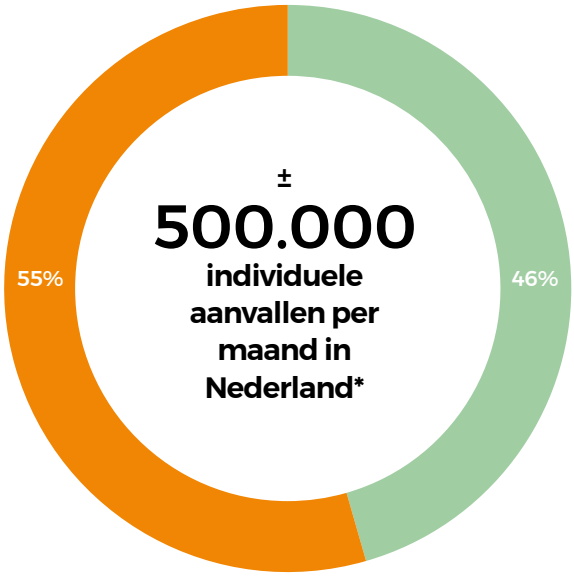
IT experts aan het woord:
"Er is toch al van alles geregeld (firewall et cetera). Ja, over het algemeen werkt de standaard beveiliging maar daar moet je niet 100% op vertrouwen, de menselijke factor speelt een rol. Van buitenaf kun je een hoop weren maar van binnenuit gebeurt er ook van alles."

"Men doet niet aan proactief gestructureerd onderzoek (dit is nodig om échte risico's boven tafel te krijgen). Er is geen sprake van degelijke risicoanalyses. Hoe dichtbij is het? Al jaren zijn er wereldwijd problemen maar dat is een ver van mijn bed show. Toen Maastricht gehackt werd kreeg men heel veel vragen. De noodzaak van IT-beveiliging wordt onderschat, financiën staan over het algemeen onder druk."

Problemen met IT-beveiliging zijn groots in aantallen en dit is relatief goed bekend maar de dreiging binnen het onderwijs wordt fors onderschat

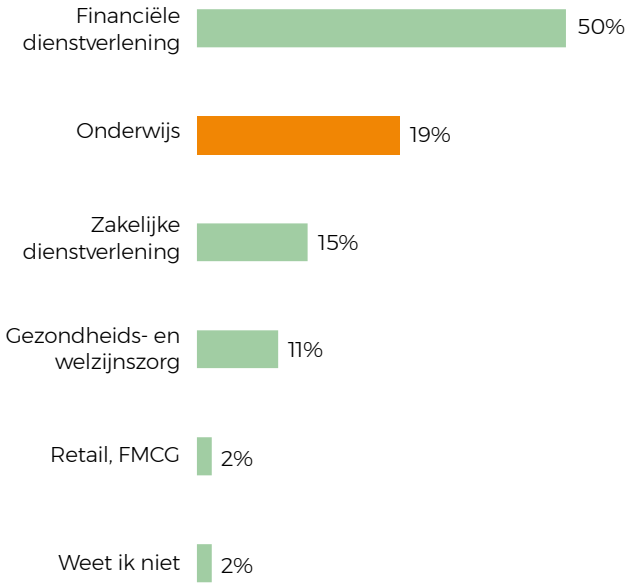
80% van de doelgroep weet **niet** dat het onderwijs veruit de meest aangevallen sector is.

Hoeveel individuele aanvallen schat u in dat er binnen een periode van 30 dagen in Nederland plaatsvinden? (n=129)



Antwoordcategoriëen:
0-100.000 | 250.000-400.000 | 400.000-600.000 | Weet ik niet

De top 3 van meest aangevallen sectoren krijgt zo'n 80% van de aanvallen te verduren. Welke sector voert volgens u deze lijst aan? (n=125)



NB: De onderwijssector staat met stip op 1 en neemt een aandeel van zo'n 60% voor haar rekening*.

Bron: microsoft.com/en-us/wdsi/threats

De onbekendheid met de dreiging binnen het onderwijs vormt samen met de alsmaar toenemende hoeveelheid van gevoelige data, een beperkt bewustzijn van impact én snel vorderende ontwikkelingen een gevaarlijk beeld voor de Nederlandse samenleving

IT experts aan het woord:
“Men heeft maar half in de gaten wat de impact van het stelen van identiteit teweeg brengt. Het onderwijs grossiert in persoonsgegevens en digitalisering vraagt erom dat er steeds meer systemen aan elkaar geplakt moeten worden. Hoe groter de materie hoe complexer het wordt (scholen worden ook groter) om een gedegen beveiliging op te zetten. Het wordt steeds aantrekkelijker om een school aan te vallen.”

“Cybercriminaliteit neemt snel toe, het is ook best lastig om hier strategie op te bepalen. Ontwikkelingen gaan in rap tempo. Het is een veelkoppig monster. Maatregelen zijn gelaagd nodig. Groot gedeelte van het VO lijkt zich nog niet echt bewust van wat er op zich af komt.”

Persbericht Autoriteit Persoonsgegevens

AP luidt noodklok: explosieve toename hacks en datadiefstal

Nieuwsbericht / 1 maart 2021 Categorie: Meldplicht datalekken

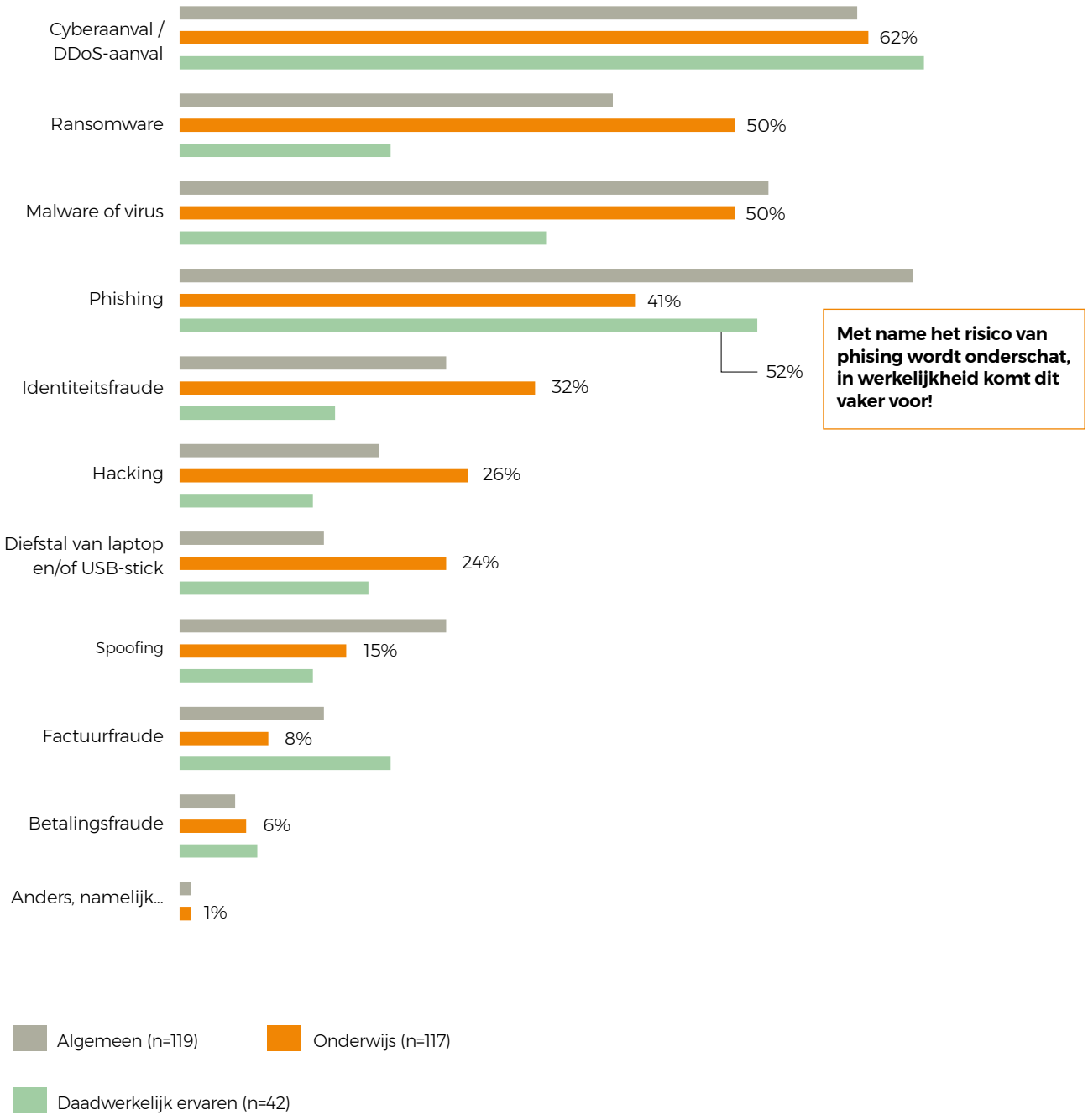
De Autoriteit Persoonsgegevens (AP) meet een explosieve toename van het aantal hacks, gericht op het buitmaken van persoonsgegevens. Het aantal meldingen steeg in 2020 met maar liefst 30% ten opzichte van vorig jaar. Datadiefstal is vaak te voorkomen door een betere beveiliging. Dat blijkt uit de 'Rapportage Datalekken 2020' die AP-voorzitter Aleid Wolfsen vandaag naar de Tweede Kamer heeft gestuurd.

DDos aanvallen grootste dreiging met als gevolg platleggen van het onderwijs. Beleid rondom IT-beveiliging is nauwelijks aangescherpt ondanks toegenomen kwetsbaarheid tijdens de pandemie.

2

DDoS aanvallen, ransomware én malware of virussen komen volgens de doelgroep op onderwijsinstellingen het meest voor en vormen daarmee ook de grootste risico's

Welke problemen op het gebied van IT beveiliging komen volgens u het meest voor? En welke vormen het grootste risico binnen het onderwijs



Men noemt spontaan grofweg drie thema's als het gaat om risico's als gevolg van problemen met IT-beveiliging

Platleggen van infrastructuur; continuïteit van het onderwijs komt in gevaar

IT-medewerker binnen het VO:
"Cryptolockers die al wat langer (inactief) in een back-up zitten. Hoe relevant is het terugzetten van een (verouderde) back-up? Verstoren van de online toegang tot clouddiensten. Steeds meer draait buiten de deur. DDOS kan processen op school ernstig verstoren."

Directielid binnen het VO:
"We hebben meerdere keren in het afgelopen jaar te maken gehad met DDos aanvallen op portals van onze leveranciers en een enkele maal op onze eigen IP adressen. En uiteraard hebben we ook mails en SMS'en gekregen die phishing betreffen. Overigens houdt onze firewall veel van dergelijke berichten tegen.

Ongeautoriseerde toegang tot data én systemen; lekken van persoonsgegevens

IT-medewerker binnen het VO:
"Risico op inzage in het leerling administratie-systeem, waardoor gegevens op "straat" liggen. Het platleggen van de infrastructuur zou desastreus zijn. De lessen kunnen dan geen doorgang vinden, zeker niet als er online lessen zijn."

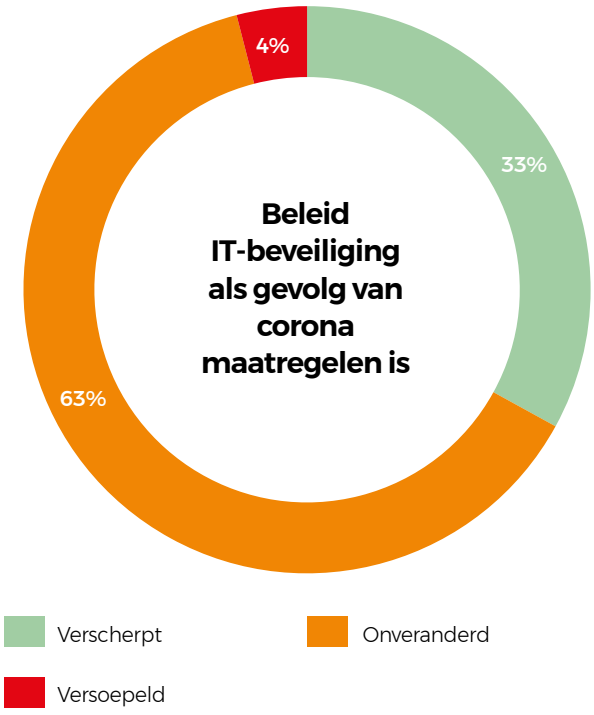
Bestuurslid binnen het VO:
"Leerlingen die in de cijfersystemen proberen naar binnen te komen, maar vervolgens ook bij mails van docenten kunnen komen.

Verkeerd gebruik van IT door medewerkers en leerlingen met diverse gevolgen van dien

CIO binnen het VO:
"Menselijke factor. Data lek veroorzaakt door te gebrekkige digitale kennis en ondoorzichtig applicatielandschap op enkele plekken waardoor slecht bekend is waar welke data is (en wat er potentieel gelekt is)."

IT-medewerker binnen het VO
"Het grootste probleem is dat gebruikers te veel informatie doorsturen. Dus niet alleen de gevraagde informatie maar het hele overzicht. Ik denk hier bij aan geëxporteerde Excel bestanden."

Toenemende druk op beveiliging binnen het onderwijs als gevolg van de pandemie zorgt bij een grote meerderheid van onderwijsinstellingen niet voor aanscherping van het reguliere beleid



IT medewerker binnen het VO:
"Corona heeft vaardigheid en daarmee bewust-wording ict enorme boost gegeven, ook op beveiliging."

Berichtgeving Dutch IT-channel

Meer DDoS-aanvallen door pandemie
Met meer mensen dan ooit online, als gevolg van de pandemie afgelopen lente en zomer, zijn netwerken het favoriete doelwit geworden voor cybercriminelen. Wereldwijd is het totale aantal DDoS-aanvallen in Q1 2020 zelfs met 80% gestegen in vergelijking met Q1 2019. De aanvallen op educatieve bronnen waren voor een groot deel verantwoordelijk voor deze groei.

Procentuele stijging in vergelijking met 2019	Januari:	Februari:	Maart:	April:	Mei:	Juni:
	550%	500%	350%	480%	357.14%	450%

Wat is er precies aangescherpt binnen uw beleid rondom IT-beveiliging als gevolg van de coronacrisis? Wat heeft nu meer focus gekregen en waarom? (n=28)

Ook binnen de groep die wel aangeeft het beleid te verscherpen lijken de acties lang niet altijd voldoende om risico's écht buiten de 'virtuele' deur te houden

Zo'n 1 op de 3 werkt enkel aan de bewustwording en instrueert personeel opnieuw. Daadwerkelijk aangescherpte controle op IT om ook buiten de schoolmuren de beveiliging op orde te houden is beperkt tot een selecte groep

IT medewerker binnen het VO:
"Aanvulling op de gedragscode voor gebruik van video-vergaderen en lesgeven op afstand met camera."

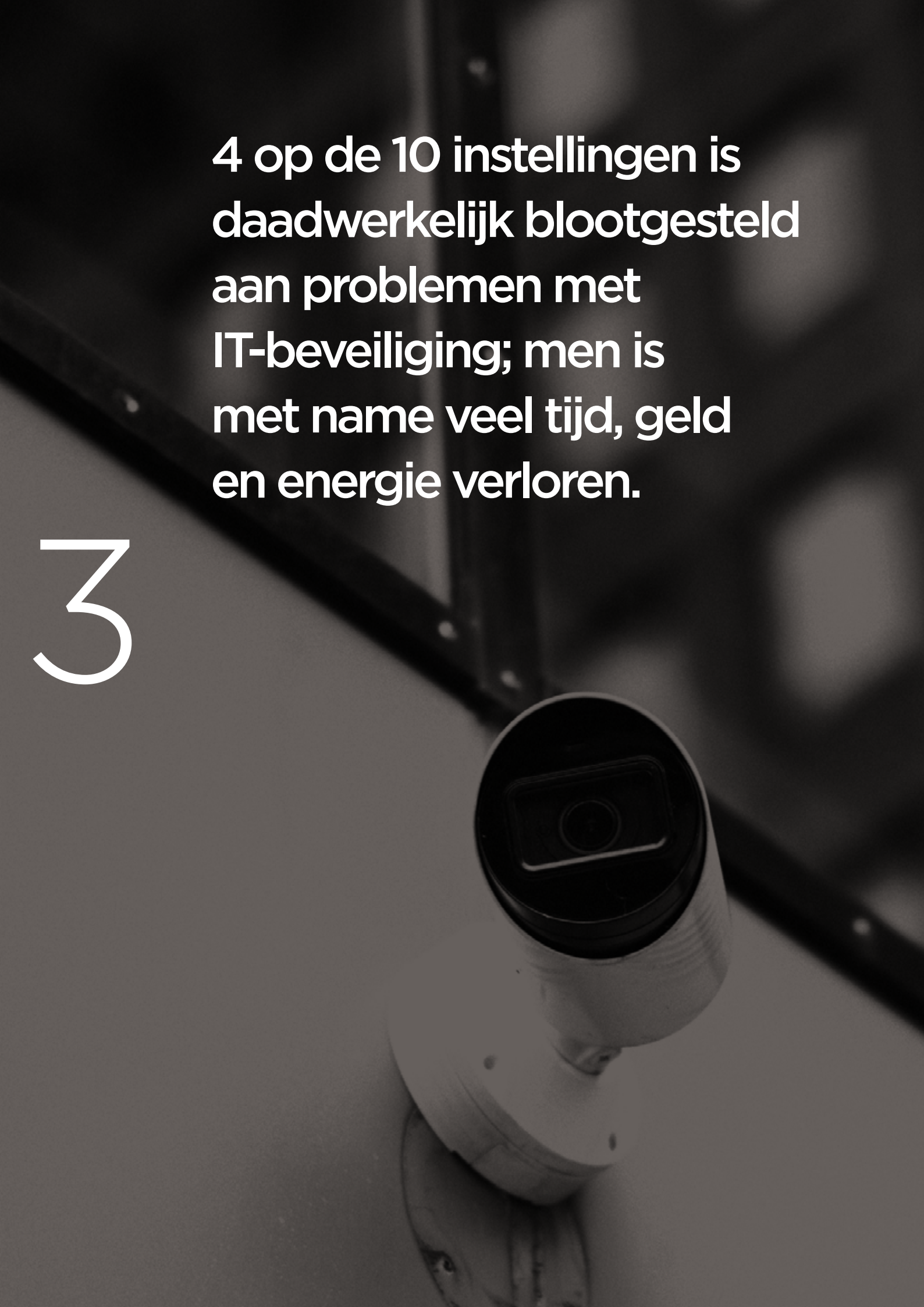
IT medewerker binnen het MBO:
"Thuiswerken kwam eerder niet/nauwelijks voor. Handelingen die daarbij horen zijn nu beschreven."

IT medewerker binnen het VO:
"Het wachtwoordenbeleid (MFA en SSO) ingevoerd doordat er steeds meer thuisgewerkt wordt en met BYOD."

CIO binnen het VO:
"Meer aandacht en beveiliging vanaf externe locaties, werken met geografische filters en dergelijke."

Directielid binnen het VO:
Diverse technische en organisatorische maatregelen genomen, o.a.: geautomatiseerd gebruikers- en toegangsbeheer door IDM koppeling met personeelsadministratie en leerling administratie. Uitbreiding multi-factor authenticatie en cybersecurity afgesloten

Wat is er precies aangescherpt binnen uw beleid rondom IT-beveiliging als gevolg van de coronacrisis? Wat heeft nu meer focus gekregen en waarom? (n=28)

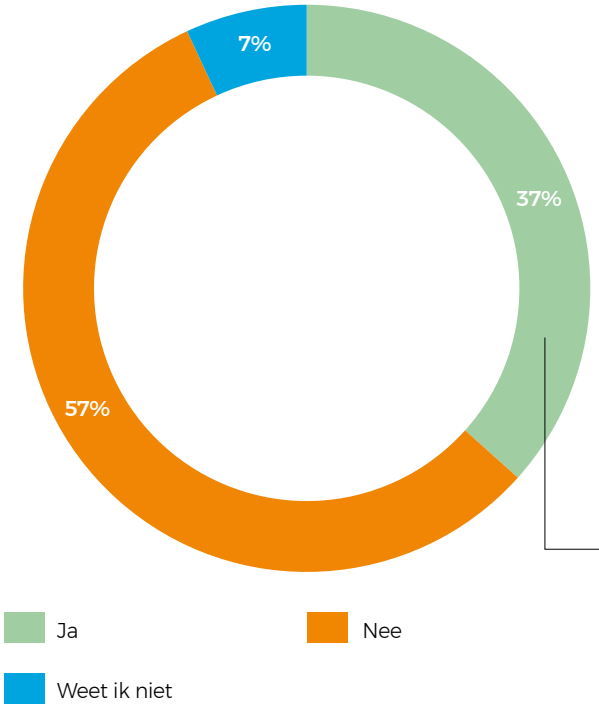


4 op de 10 instellingen is daadwerkelijk blootgesteld aan problemen met IT-beveiliging; men is met name veel tijd, geld en energie verloren.

3

Bijna vier op de tien onderwijsinstellingen heeft in het afgelopen jaar te maken gehad met problemen op het gebied van IT-beveiliging

Heeft u in het afgelopen jaar te maken gehad met problemen op het gebied van IT beveiliging (n=115)



Het bestuur, de directie en evt. de CIO meent vaker last te hebben van problemen (56%) dan de IT medewerker (31%).

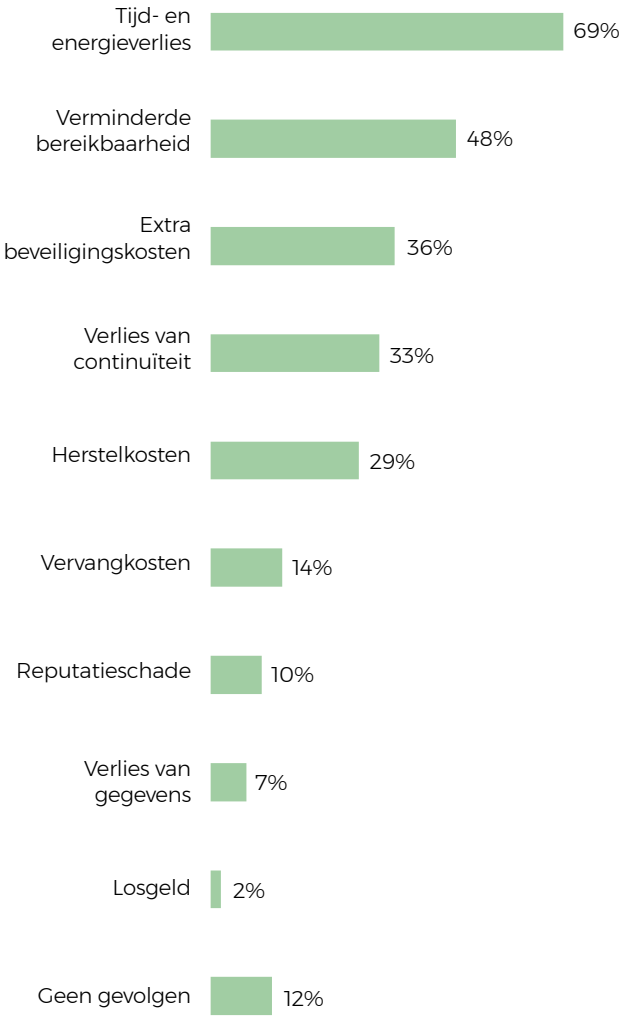
Mogelijke interpretatie van verschil in beleving:

IT medewerker binnen het VO:
"Een DDoS aanval komt vrijwel iedere dag voor, dit hebben we echter goed op orde. Het verstoord de dagelijkse werkzaamheden niet meer. 37% is naar mijn mening weinig maar persoonlijk denk ik niet aan DDoS aanvallen bij deze vraag, daar lig ik niet (meer) wakker van. Er wordt overal wel aan de deur gerammeld. Het is eerder het 'gevoel' dat er niets is gebeurd."

Basis bestuur, directie, CIO = 41, IT medewerker = 49. Beiden indicatief n < 50.

Instellingen die daadwerkelijk een aanval hebben ervaren spreken naast de continuïteit en bereikbaarheid vooral over de investeringen in tijd, geld en energie die gepaard gaan met het herstel na problemen met IT-beveiliging

Welke gevolgen heeft dit gehad voor de onderwijsinstelling?
(basis groep die aangeeft problemen ervaren te hebben, n=42)



Kunt u het voorval eens in uw eigen woorden omschrijven:

CIO binnen het voortgezet onderwijs (VO):
"Onze school heeft sinds september 2019 met regelmaat last van DDoS-aanvallen. Gevolgen zijn dat verscheidene lessen beperkt tot geen doorgang kunnen vinden, administratief medewerkers web diensten en allerlei applicaties niet kunnen gebruiken enz. Kortom: een extreem verstorende actie waar de hele organisatie last van heeft." CIO

CIO binnen het MBO:
"Wijzigen bankrekeningnummer van medewerkers".

CIO binnen het VO:
"Alle leerlingen op een locatie hebben een mail ontvangen met verzoek om bitcoins te betalen."

Bestuurslid binnen het VO:
"DDoS aanvullen die ervoor gezorgd hebben dat we de hele IP range van het interne netwerk om moesten zetten naar een nieuwe range."

Indicatieve cijfers n<50 !

Meerderheid stelt dat het aan het bestuur of de directie is om verantwoordelijkheid te nemen voor de problemen die spelen op het gebied van IT-beveiliging

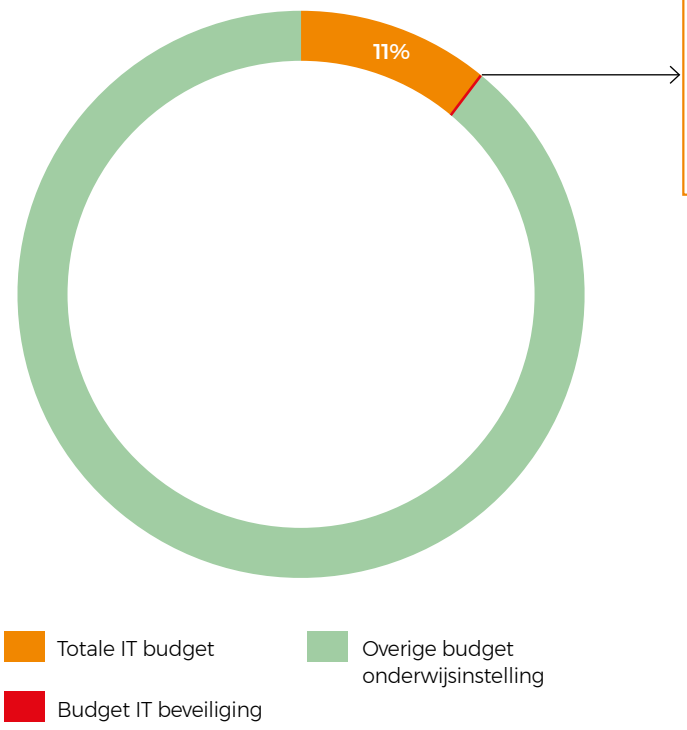
Bestuurs- en directieleden delen deze mening en plaatsen het onderwerp hoog op de agenda. In de praktijk wordt er door de meerderheid van de onderwijsinstellingen 5% of minder van het IT-budget budget toegewezen aan IT-beveiliging:

77%

stelt directie danwel de voorzitter van RvB eindverantwoordelijk voor IT-beveiliging

Welk percentage van het totale budget dat uw onderwijsinstelling te besteden heeft is gereserveerd voor IT? (n=95)

En hoeveel daarvan is gereserveerd voor IT beveiliging? (n=95)



Voor zo'n 2 op de 3 onderwijs-instellingen gaat er 5% of minder van het IT-budget naar IT-beveiliging

Wie is er volgens u eindverantwoordelijk voor IT-beveiliging binnen uw onderwijsinstelling? (n=99)

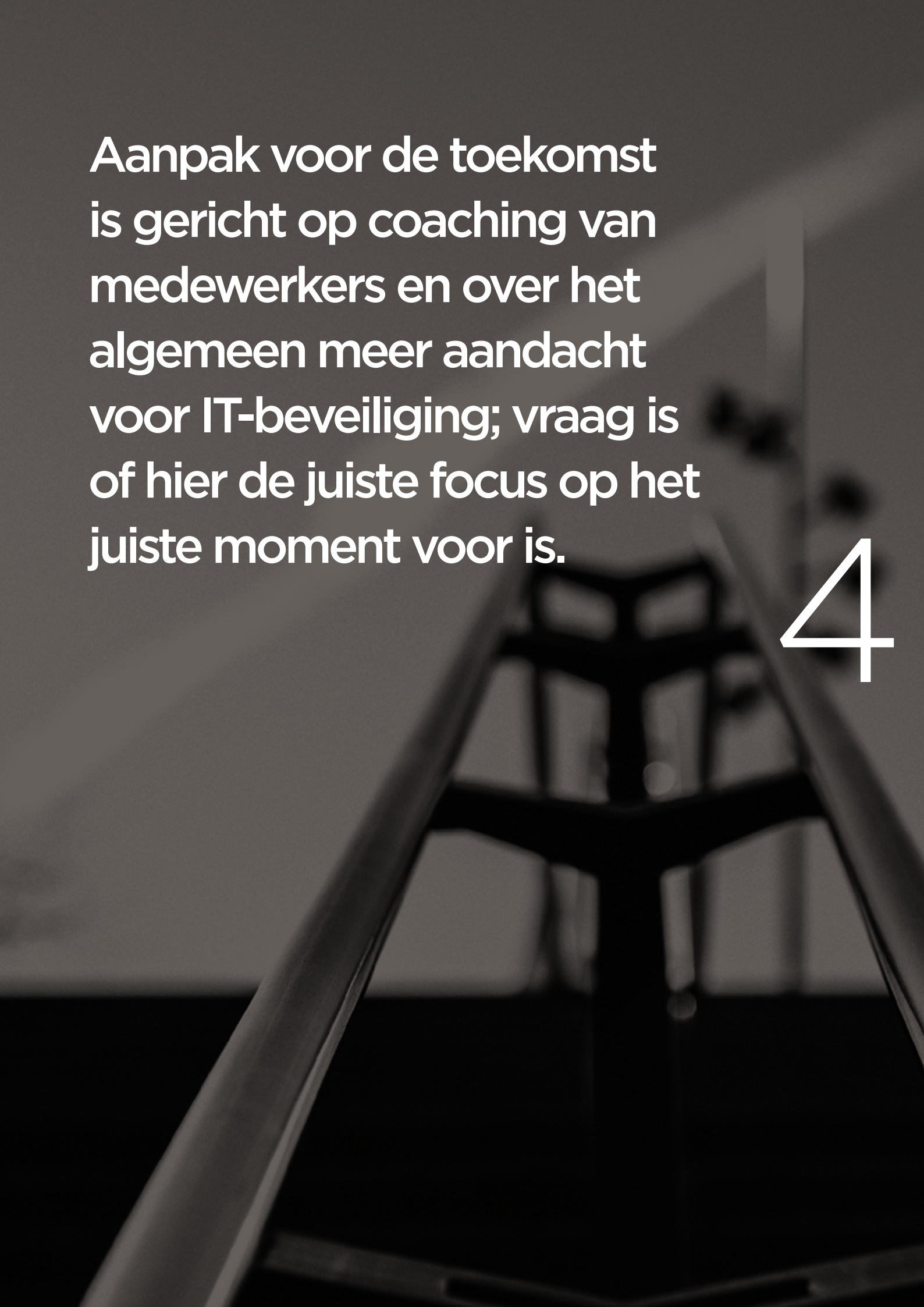
IT experts onderschrijven dat bestuur en directie (enig) belang hechten aan IT-beveiliging maar in de praktijk blijft een gedegen aanpak regelmatig (lang) uit

“Het onderwijs zou je kunnen omschrijven als grote olietanker die je vrij moeilijk van koers kan veranderen. Er gaat veel tijd én energie in zitten.”

“De wens is er om er iets mee te doen maar het concretiseren van een IT aanpak kost meer tijd en moeite.”

“IT medewerkers zijn flink met beveiliging bezig, zij willen het een plaats geven, Standaard dingen zijn over het algemeen goed geregeld maar het grootste probleem zit bij gebruikers. Alertheid op zaken die niet kloppen is essentieel. Zolang het bestuur of de directie binnen de instelling deze ontwikkelingen (NB: daadwerkelijke problemen binnen de eigen instelling) niet ervaart blijft het een lastig punt om op de agenda te houden.”

“Een preventieve aanpak is van groot belang. Indien je het niet doet neem je bewust een aantal risico’s. Het gaat nu allemaal goed en dat wil je zo houden maar de ontwikkelingen gaan heel snel.”

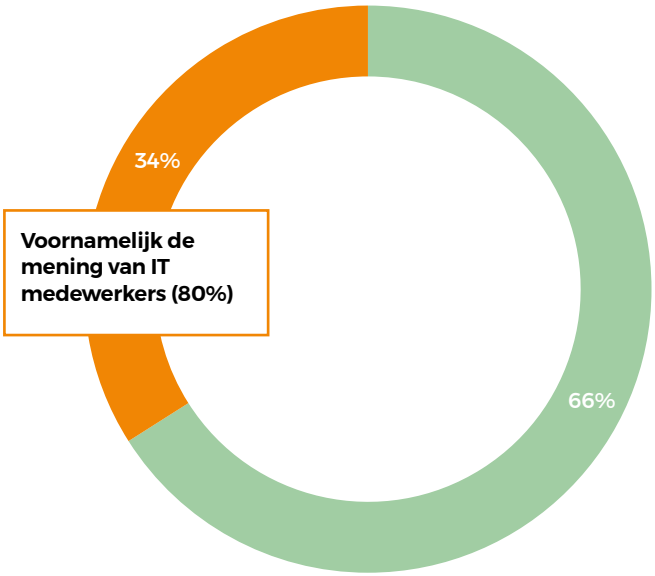


Aanpak voor de toekomst is gericht op coaching van medewerkers en over het algemeen meer aandacht voor IT-beveiliging; vraag is of hier de juiste focus op het juiste moment voor is.

4

Meerderheid van de scholen doet aan enige vorm van preventieve communicatie, initiatieven zijn zeer uiteenlopend en daarmee wellicht ook wisselend effectief

Heeft uw onderwijsinstelling een actieve communicatieaanpak met als doel preventie door bewustwording van risico's en het tonen van voorbeeldgedrag als het gaat om IT beveiliging? (n=96)



Wat voor communicatievormen past de onderwijsinstelling waar u werkt toe om medewerkers en leerlingen te betrekken bij IT-beveiliging? (n=51)

It medewerker binnen het VO:
"Na 3 maanden is een inzet van half uurtje training voor 99% weer verdwenen. Er is meer nodig, continu herinnering aan het belang van aandacht voor veilig gebruik van IT. Updates over incidenten in nieuwsbrieven. Pamfletten et cetera."

Directielid binnen het VO:
"Online cursus 'Veilig en bewust'".

IT medewerker binnen het VO:
"intranet, mails en een week met extra aandacht"

Bestuurslid binnen het VO:
"Regelmatig in nieuwsbrieven naar personeel, incidenteel naar leerlingen en ouders."

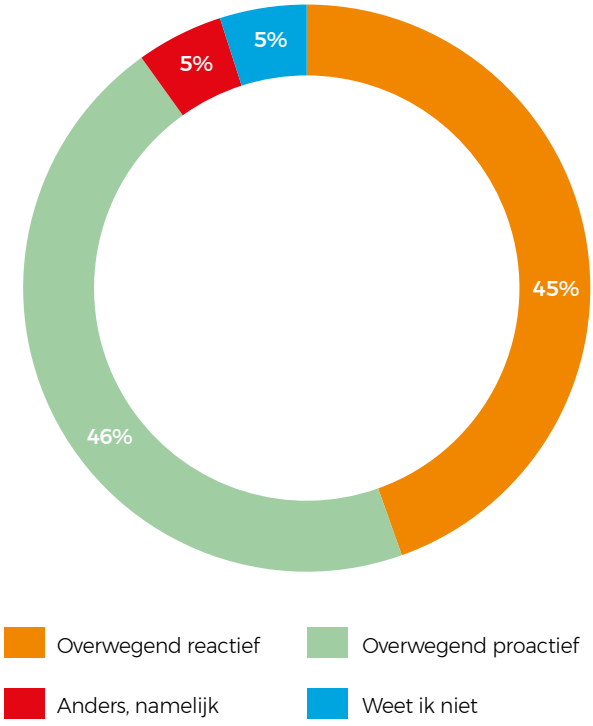
Directielid binnen het VO:
"Op studiemiddagen, in de wekelijkse nieuwsbrief komt dit onderwerp frequent aan de orde. Ook wordt er jaarlijks een AVG-handboek door alle medewerkers ondertekend."

IT-medewerkers zijn kritischer over het bestaan van een actieve communicatie aanpak gericht op preventie van problemen met IT-beveiliging

Verschil in belang en de mate van urgentie die gevoeld wordt tussen de verschillende doelgroepen binnen een onderwijsinstelling komt hier tot uiting in de praktijk.

Als het gaat om informatie-verstrekking is de houding vrijwel gelijk verdeeld over een reactieve vs. een proactieve aanpak

Hoe zou u de informatieverstrekking rondom incidenten met IT beveiliging binnen uw onderwijsinstelling over het algemeen karakteriseren? (n=107)



CIO binnen het VO:
"Er gebeurt wel een en ander maar de diverse management teams hebben veel moeite dit onderwerp voldoende te begrijpen om het dito urgentie/prioriteit te geven. Een belangrijk aandachtspunt."

IT-medewerker binnen het MBO:
"Er is nog te veel achterstallig onderhoud gaande waardoor de capaciteit niet bestaat. Het is wel een van de zaken die op de rol staan."

IT medewerker binnen het VO:
"Heeft geen prioriteit en er is geen duidelijk beeld van het belang. Men vindt dat er geen problemen zijn."

CIO binnen het VO:
"Tijd en geld te weinig. Merendeel grenst aan gedrag en algemene informatiebeveiliging en privacy (IBP) en hoort organisatorisch tezamen met communicatie/PR en privacy officers uitgezet te worden. In de praktijk is dat altijd het ondergeschoven kindje."

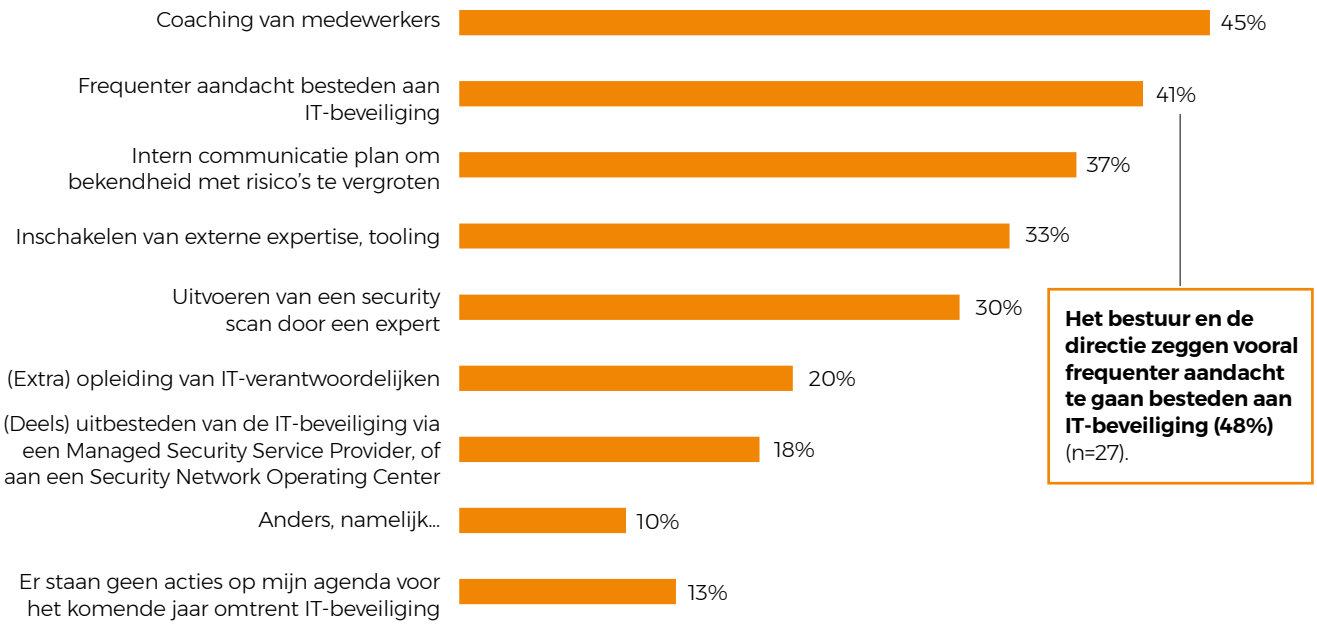
Directielid binnen het VO:
"Voornamelijk het ontbreken van budget hiervoor, wordt niet gezien als een een primaire aangelegenheid mede daardoor."

CIO binnen het VO:
"Het is de visie van het bestuur."

Waarom betrekt de onderwijsinstelling waarvoor u werkt medewerkers en leerlingen (nog) niet actief bij IT-beveiliging? (n=14)

De voorgenomen planning van een flink deel van de onderwijsinstellingen richt zich op belangrijke verbeterpunten; coaching van medewerkers en een toegenomen mate van aandacht voor IT-beveiliging (nog iets meer onder eindverantwoordelijken)

Er zijn verschillende manieren om actie te ondernemen en onderwijsinstellingen (beter) te beveiligen als het gaat om IT. Welke van de volgende items staan er bij uw onderwijsinstelling het komende jaar op de agenda? (n=92)

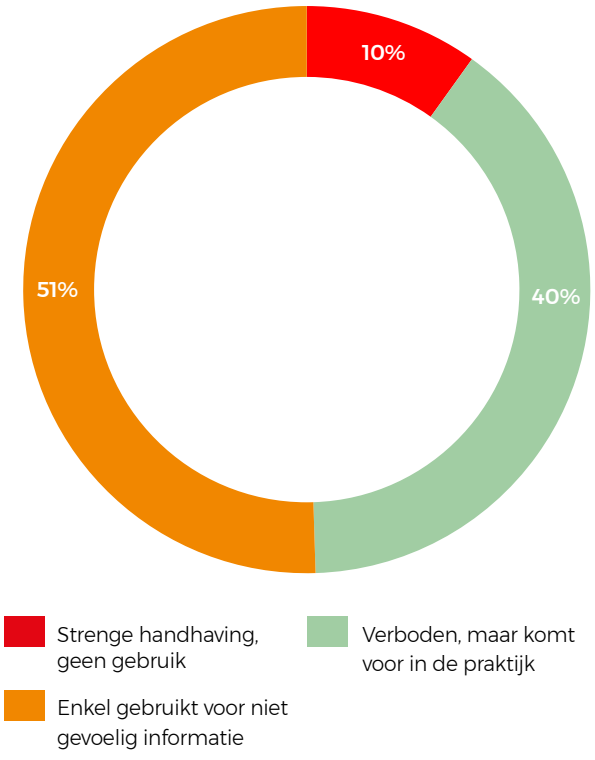


Noodzaak is hierbij dat IT-beveiliging in de juiste vorm wordt opgepakt; bewustwording van risico's door het uitvoeren van preventieve analyses lijken naast het (blijven) sturen van medewerkers en leerlingen het belangrijkst. Dialoog met de IT-medewerkers is van groot belang.

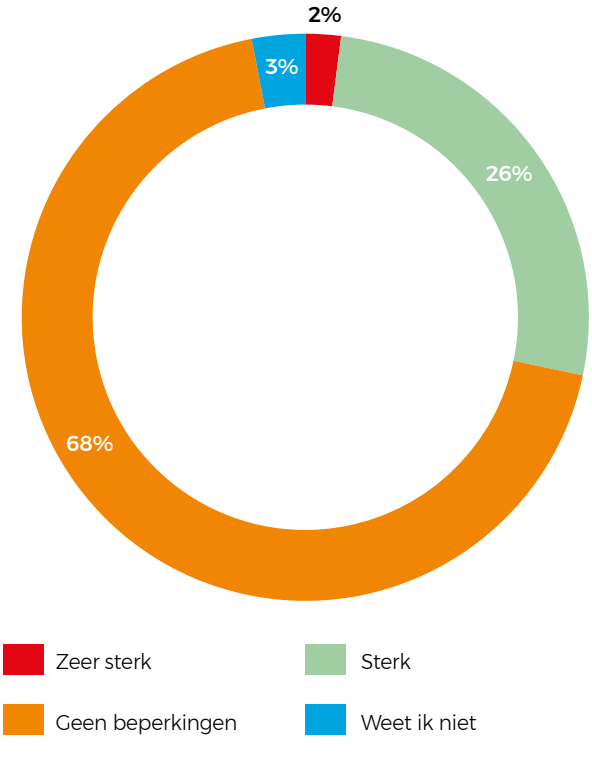
Coaching gericht op bewustwording is een eerste goede stap, daarentegen lijkt er ook noodzaak tot een dialoog

40% ziet dat beleid omtrent IT-beveiliging in de praktijk niet wordt nageleefd door leerlingen en/of medewerkers. Men stelt echter wél dat er vrijwel geen sprake is van beperkingen in de flexibiliteit van die groep als gevolg van IT-beveiliging; een mismatch

Bent u op de hoogte van risico's die het gebruik van publiek toegankelijke diensten door uw medewerkers met zich mee brengen? Denk hierbij bijvoorbeeld aan Google Drive, WeTransfer , Dropbox et cetera (n=93)

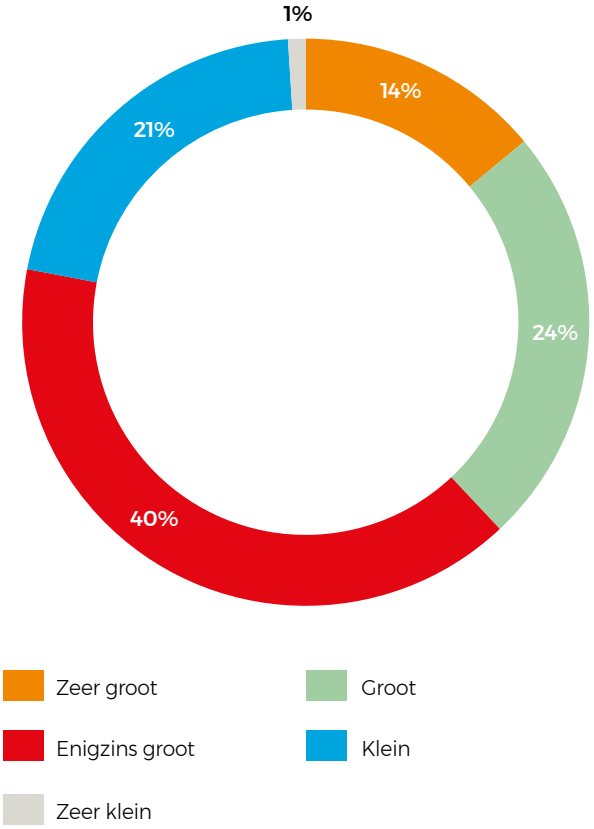


In welke mate beperkt de beveiliging van uw systemen de flexibiliteit van uw medewerkers in de dagelijkse praktijk? (n=95)

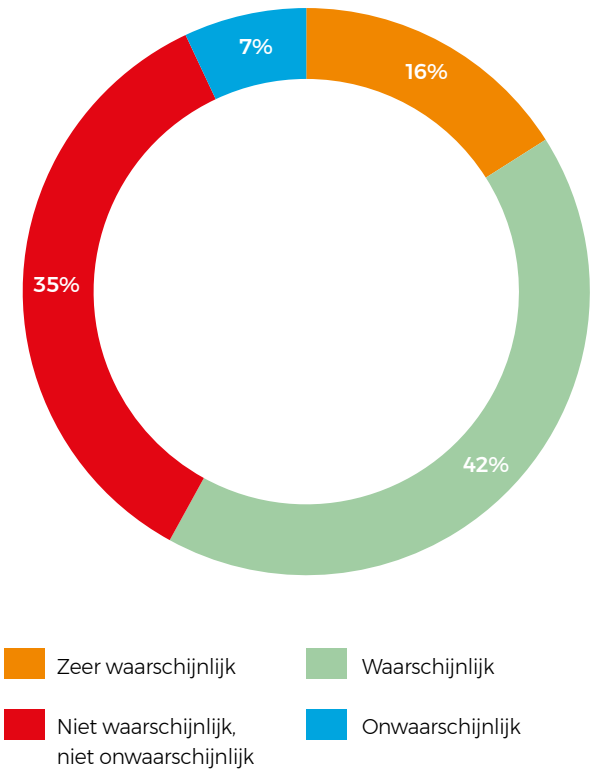


Actiegericht werken én meer budget zou voor de meerderheid van instellingen voorhanden moeten zijn; het is daarbij zaak dat de aandacht voor IT-beveiliging leidt tot acties en investeringen op het juiste moment én met de juiste focus

Hoe groot is de bereidheid binnen uw onderwijsinstelling om op korte termijn acties uit te voeren tegen aanvallen op uw IT-netwerk? (n=92)



Hoe waarschijnlijk is het dat de onderwijsinstelling waar u werkt het komende jaar (meer) investeert in IT-beveiliging? (n=92)



Bijlage

5

Gehanteerde omschrijving voor diverse type aanvallen

DDoS / Cyberaanval:	'Poging om een website onbruikbaar te maken door de server te overbelasten (bijv. DDoS-aanval)
Ransomware:	'Malware die uw netwerk, computer of bestanden 'gevangen houdt' tot u losgeld betaalt'
Hacking:	'Inbraak in uw computersysteem of netwerk om gegevens te stelen'
Identiteitsfraude:	'Illegaal gebruik van persoonsgegevens (bijvoorbeeld voor het verkrijgen van producten en diensten of het aanvragen van bankrekening of creditcard)'
Malware:	'Kwaadaardige software die een computer of netwerk verstoort (bijv. virus, trojaans paard of spyware)'
Phishing:	'Via e-mail of een vervalste website vragen naar persoonlijke gegevens, zoals inloggegevens of pincode'
Betalingsfraude:	'Virus dat criminelen in staat stelt alles op een computer te volgen en geld weg te sluizen van rekeningen'
Factuurfraude:	'Het vervalsen van facturen. Een oplichter onderschept een factuur. Hij wijzigt daarop alleen het rekeningnummer. Degene die de rekening betaalt, maakt (zonder het te weten) geld over naar de fraudeur in plaats van naar het bedrijf dat de nota verstuurt.'
Spoofing:	Het vervalsen van kenmerken met als doel om tijdelijk een valse identiteit aan te nemen

Onderzoeksverantwoording

Onderzoeksperiode	Het veldwerk heeft gelopen vanaf woensdag 27 januari t/m vrijdag 12 februari 2021
Onderzoeksdoelgroep	In dit onderzoek ondervragen wij personen werkzaam binnen het voortgezet en MBO onderwijs in Nederland. Daar binnen richten wij ons specifiek op bestuursleden (of directie bij een kleinere school), en de CIO / IT afdeling
Steekproefbron	De steekproef is aangeleverd door Breens. Resultaten zijn niet gewogen.
Steekproefgrootte	In totaal was een steekproef van 1707 personen aangeleverd. Hiervan hebben 129 gereageerd op de vragenlijst (89 volledig ingevuld en 40 deels; 7 Bestuurslid CIO, 20 Directielid, 14 CIO en 49 IT-medewerker)
Onderzoeksmethode	Respondenten zijn via e-mail benaderd voor deelname aan de online vragenlijst. Gedurende het veldwerk zijn er 2 reminders gestuurd
Vragenlijstlengte	Vragenlijst bestond uit verschillende onderwerpen m.b.t. IT/Cyber security (perceptie, status quo, behoefte en achtergrondvariabelen) en had een gemiddelde vragenlijstlengte van 11 minuten
Verdiepende interviews	Op 18 en 19 februari zijn er telefonische interviews gehouden met een drietal IT experts (aangedragen door Breens) om de resultaten verder te duiden én rijke praktijkvoorbeelden op te halen.


breens network