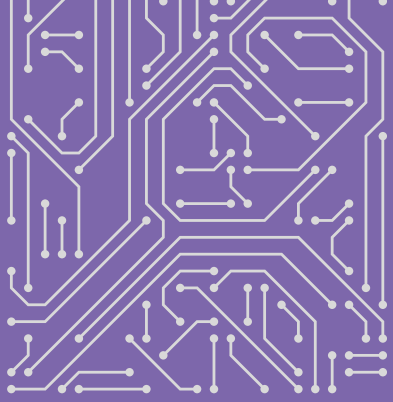


kien

Samen ICT *voor onderwijs*

WHITEPAPER

PHISHING IN HET ONDERWIJS

EEN SNOEPWINKEL VOOR HACKERS

LOOPT HET ONDERWIJS RISICO?

Het risico op phishing wordt binnen het onderwijs onderschat. In werkelijkheid komt dit vaker voor dan men denkt. p.6

LAATSE VERDEDIGINGSLINIE

Een belangrijke rol in het veilig houden de digitale schoolomgeving ligt bij medewerkers. p.4

www.kienict.nl

Het onderwijs ligt onder vuur

De combinatie van afstandsonderwijs met contactonderwijs heeft een grote druk gelegd op de schouders van zowel de leerkrachten, die meerdere ballen tegelijk in de lucht moeten zien te houden, als het administratief en technisch personeel, die ervoor instaan dat iedere leerling toegang heeft tot de verschillende soorten lessen, oefeningen en toetsen.

Als gevolg van de coronapandemie hebben we nieuwe digitale hulpmiddelen leren kennen, op de werkvloer en op school. Deze digitale hulpmiddelen blijven een onmiskenbare rol spelen in ons professionele leven en zullen dit ook in de toekomst blijven doen. Dit brengt gevaren met zich mee waar we vandaag, en in de toekomst, mee moeten leren omgaan.

+18%

Toename cyberaanvallen

Volgens onderzoek steeg het aantal cyberaanvallen op onderwijsinstellingen het afgelopen jaar met 18%. Dat is meer dan in iedere andere sector.

Waarom gericht op onderwijs?

Dat doet de vraag rijzen waarom hackers zich zo graag op onderwijsinstellingen richten? Daar gaan we in dit whitepaper dieper op in. We bekijken wat de aantrekkingskracht is, niet alleen van hogescholen en universiteiten, maar ook van middelbare-, voortgezet en basisscholen.

Een schatkist aan informatie

Het onderwijs is geen rijke sector maar wel zeer 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 onderzoeksproject enz. Met deze data valt een hoop geld te verdienen. Daarom vinden de meeste cyberaanvallen in het onderwijs plaats. Jouw school vormt een schatkist aan informatie voor cybercriminelen. Een ware snoepwinkel.

Hoe meer informatie een hacker tot zijn beschikking heeft, hoe groter de kans op een geslaagde phishingaanval.
Universiteiten zijn met name interessant voor de hackers vanwege hun onderzoeksdata. Bij hogescholen, middelbaar-, voorgezet- en zelfs basisonderwijs speelt met name de schat aan (persoonlijke) informatie van leerlingen en studenten een grote rol. Denk hierbij aan: e-mailadressen, geboortedata, informatie over gezins- en financiële situatie en nog veel meer.

Zodra de hacker binnen is in het netwerk van een school, dan loopt iedereen gevaar: medestudenten, leraren, technisch en administratief personeel, enz. Dat gaat als volgt: een student ontvangt een phishingmail, klikt op een malafide link en vult zijn inloggegevens in. Vervolgens stuurt de hacker een gepersonaliseerde mail naar een leraar die eveneens vanuit zijn goede bedoelingen om de student te helpen, in de val trapt. Na enkele gevallen van dergelijke spear phishing loopt al snel een hele afdeling gevaar.

'Het onderwijs grossiert in persoonsgegevens'

Basis- en voorgezet onderwijsscholen worden veelal slachtoffers van hackers als gevolg van een breed verspreide aanval die zoveel mogelijk slachtoffers probeert te maken. Hackers komen binnen bij de organisatie die het meest toegankelijk is. Eenmaal binnen, kunnen hackers hun nep e-mailcampagne snel verspreiden binnen het hele schoolnetwerk. Eén nep-mail kan hierdoor een grote gevolgen hebben.

De gevolgen van een cyberaanval 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.

Kun je phishing voorkomen?

Het 'Phishing per brancherapport 2020' dat werd gepubliceerd door KnowBe4 stelde dat mensen die in het onderwijs werkten, niet voldoende waren opgeleid om phishing-schema's te identificeren en aan te pakken wanneer ze deze tegenkwamen. Volgens het rapport waren werknemers in het onderwijs het meest geneigd om ten prooi te vallen aan phishing en social engineering-tactieken van alle andere werknemers in andere sectoren, behalve in de gezondheidszorg. Het goede nieuws is dat training voor hen werkt. Nadat de medewerkers voldoende waren opgeleid, daalde het aantal mislukkingen voor de phishingtest van 30% naar 5%.

Om phishing te kunnen voorkomen is het belangrijk dat medewerkers weten hoe ze een phishingmail kunnen herkennen. Wanneer kunnen ze wel en wanneer niet op die link klikken. Nu we weten dat training werkt kan het het versturen van phishingsimulaties een goed middel zijn om de kennis van medewerkers hierover te vergroten. Deze simulaties zijn immers gebaseerd op echte in de praktijk voorkomende phishingmails. De phishingsimulaties zijn dan ook bedoeld om te leren echte phishingmails te herkennen.

Zwakke schakel of laatste verdedigingslinie?
Uit onderzoek naar het uitvoeren van phishingsimulaties is door onze leverancier van phishingsimulaties, Phished, gebleken dat iedere medewerker even vatbaar is voor phishingmail, ongeacht welke functie de medewerker heeft. Bij een eerste test gaat steevast (minstens) 1 op de 5 in de fout. Als 20 procent van 500 medewerkers van een onderwijsinstelling ingaat op een phishingmail, kom je als snel aan bijna 100 mogelijke ingangen. Zodra een hacker binnen zit, krijg je hem heel moeilijk weer naar buiten.

Het gaat de hacker niet altijd om de mogelijke winst via losgeld of verkoop van de data. Iemand die leerlinggegevens in handen krijgt, heeft een houdgreep op het leven van die (vaak nog jonge) leerlingen of studenten in een kwetsbare fase van hun ontwikkeling. Het zet de deur open naar discriminatie, pesten, identiteitsfraude, etc.

Wiens schuld is het?
Wanneer een onderwijsinstelling wordt geconfronteerd met ransomware, wordt vaak gekeken richting KIEN als ICT-ondersteuner. Deze medewerkers beheren de systemen, staan in voor het up-to-date en veilig houden van die systemen en de netwerken. Het is echter niet mogelijk om de systemen helemaal dicht te zetten, omdat medewerkers dan hun werk niet meer kunnen doen. Helaas wordt er, als het mis gaat, toch vaak naar de rol van ICT gekeken.

Dat is niet terecht. Met name in het geval van phishing is het voor een hacker genoeg om toegang te krijgen tot het netwerk via een standaardaccount met weinig rechten, ondanks alle technische maatregelen die KIEN kan nemen is een 'klik' op een link zo gebeurd. Van daaruit kan een hacker zich verder bewegen in de systemen en zich een weg omhoog werken. Iedere medewerker moet daarom doen wat mogelijk is.

Hieruit blijkt wel dat iedereen zijn steentje bij moet dragen om te zorgen voor een veilige omgeving. Een medewerker dient er voor te zorgen dat hij voldoende geïnformeerd is en weet hoe er veilig gewerkt kan worden en de schoolorganisatie dient er voor te zorgen dat deze informatie beschikbaar is en dat er voldoende technische maatregelen genomen worden. **Jij bent de laatste verdedigingslinie!**

Valse links herkennen

Het goed kunnen afwegen of je een e-mail veilig kunt openen is makkelijker gezegd dan gedaan. Het is vaak erg moeilijk om valse e-mails te herkennen, vooral als het gaat om gerichte aanvallen. Hieronder vind je een aantal voorbeelden om mogelijke valse e-mails te herkennen.

Punt, domeinnaam, schuine streep

Een correct webadres bestaat uit de naam van het bedrijf, gevolgd door een punt en daarna vaak nl of soms com. Samen wordt dit de domeinnaam genoemd. De domeinnaam vind je altijd direct vóór de eerste enkele schuine streep. Controleer of dit de juiste naam is van de website waar naar volgens verwachting verwezen moet worden.

https://www.kienict.nl/kien-ict/

- Check of de domeinnaam juist is: kienict.nl
- Extra tekst vóór de domeinnaam gescheiden met punt
- Extra tekst achter de domeinnaam gescheiden door een schuine streep (‘/’)

https://www.consumentenbond.nl/veilig-internetten/

- Domeinnaam: consumentenbond.nl
- Extra tekst voor domeinnaam gescheiden met punt
- Extra tekst na domeinnaam gescheiden door schuine streep

https://login-consumentenbond.nl

- Geen punt voor domeinnaam

https://abnamro.nl.nieuwsbrief2022.nl

- Geen schuine streep (‘/’) achter domeinnaam abnamro.nl

Onderwijs onderschat dreigingen

Phishing in het onderwijs wordt vaak onderschat. Gezien de vele cyberaanvallen en het aantal geslaagde cyberaanvallen in het onderwijs de afgelopen jaren, vormt deze onderschatting een risico. Het lijkt wel alsof mensen het eerst moeten meemaken voordat ze inzien hoe kwetsbaar ze zijn. Dat is ook de reden dat jouw onderwijsinstelling heeft besloten om KIEN phishing simulaties te laten doen.

Zo krijg je als medewerker heel concreet te maken met phishing en ondervind je hoe het eraan toegaat wanneer zo'n aanval succesvol is. Bij de eerste phishingsimulatie klikten 35% van de ontvangers op de link in de mail. Dit is meer dan het landelijk gemiddelde van 20%. Het onderwijs scoort hierin helaas slechter dan gemiddeld, volgens onderzoek.

De ervaring leert dat, ondanks dat het een simulatie phishingmail is, en er dus geen data of systemen echt gevaar liepen, deze testen vaak toch wat tumult veroorzaken. Mensen maken zich zorgen en de helpdesk van KIEN krijgt veel vragen.

De impact blijft ook daarna nog aanwezig. Ook omdat je weet dat er regelmatig een simulatiephishingmail zal komen. Medewerkers worden hierdoor veelal alerter en herkennen eerder een phishingmail, ook een echte phishingmail, wat uiteraard het belangrijkste is. Hopelijk draagt dit bij aan het beseft hoe makkelijk een echte phishingmail in je mailbox terecht kan komen. Hierdoor beperken we met zijn allen het risico op onderschatting van een phishingmail.

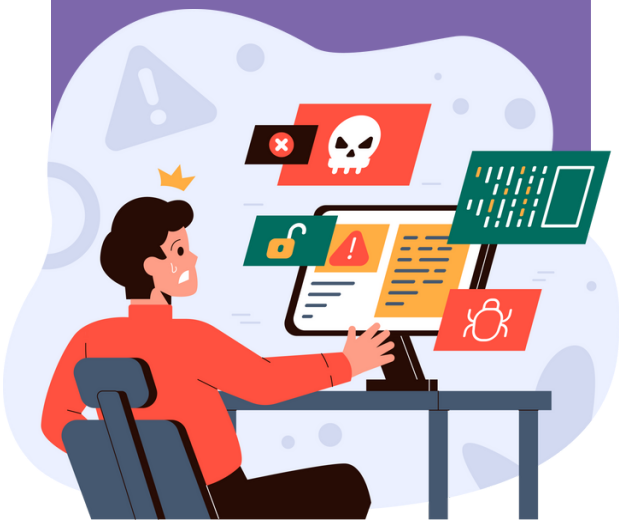
5% of minder van het IT-budget wordt in het onderwijs besteed aan privacy en security tegenover 26-29% in het bedrijfsleven. Zet dit af tegen het feit dat 60% van alle cyberaanvallen is gericht op het onderwijs en het feit dat het onderwijs grossiert in persoonsgegevens en werkt in een tamelijk open omgeving door een grote en diverse groep aan gebruikers.

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

Een hack wordt een datalek

De meest voorkomende digitale dreigingen komen nog steeds van massacampagnes die zoveel mogelijk slachtoffers proberen te maken. Denk aan de zogenaamde mail van een directeur aan een administratieve medewerker met de vraag de factuur te controleren. Als die in grote getale verstuurd wordt naar veel medewerkers, is er altijd wel iemand die in de phishingmail trapt. Daarnaast komt spearphishing ook steeds vaker voor. Dit zijn gerichte mails op basis van informatie die hackers vinden in personeelsbestanden of deze informatie afhalen van jouw sociale media account. In deze gevallen worden ook de namen genoemd van de mensen waarvan je de e-mail verwacht, waardoor deze nog moeilijker te herkennen zijn.

"De laatste verdedigingslinie ben je zelf."



Cybersecurity, waaronder weten hoe je veilig kunt werken, speelt dus een belangrijk rol voor de bescherming van persoonsgegevens. Om de gegevens van onze leerlingen, studenten en medewerkers goed te kunnen beschermen volgens de regels van de Privacywet is een beschermde en daarmee veilige omgeving noodzakelijk. Als een hacker door de beveiliging heen komt, dan kunnen de persoonsgegevens van jouzelf maar ook die van leerlingen/studenten gestolen worden. In veel gevallen worden deze persoonsgegevens daarna verkocht op het dark web. Dan is een datalek het directe gevolg van een hackingaanval. Het is daarom belangrijk om te voorkomen dat een hacker binnenkomt. Besef dat je als medewerker een belangrijke rol speelt als laatste verdedigingslinie bij het veilig houden de digitale schoolomgeving.

Toename van digitalisering betekent toename van risico

Nu de digitalisering van de schoolomgeving steeds belangrijker wordt en er geen les meer gegeven kan worden zonder de digitale schoolomgeving, nemen ook de risico's steeds meer toe. Scholen moeten daarom altijd op hun hoede blijven voor mogelijke cyberaanvallen. Het wordt daarmee nog belangrijker om te zorgen voor een goede cyberweerbaarheid bij leerlingen en medewerkers en het nemen van technische maatregelen.

Geen digitaal onderwijs zonder digitale veilig- en vaardigheid

Iedereen is verantwoordelijk voor digitale veiligheid

De ministers van onderwijs zien ook het grote belang van digitaal onderwijs. Zij hebben in de zomer van 2022 hierover een brief aan de Tweede Kamer geschreven. In de brief geven ze aan dat het belangrijk is dat elke leerling en student in een veilige omgeving onderwijs kan volgen. Dit geldt niet alleen voor het fysieke gebouw maar ook in het digitale domein dat steeds meer deel uitmaakt van het onderwijs. Digitale veiligheid is niet alleen iets voor de ICT-verantwoordelijke, maar een verantwoordelijkheid van de hele school, van het bestuur tot en met de leraar in de klas.

"Digitale veiligheid is een voorwaarde voor digitaal onderwijs."

We beschermen er niet alleen onze eigen persoonlijke gegevens mee, maar ook die van alle collega's, leerlingen en studenten. Zoals in deze whitepaper duidelijk is geworden vormt met name een fenomeen als phishing een gevaar in deze tijd. Laten we er daarom samen aan werken om phishingmails te kunnen herkennen, zodat we een sterke laatste verdedigingslinie vormen met onze collega's.

Continu bijleren en veranderen

Door de frequentie van veranderingen in digitale hulpmiddelen, organisatie, maatschappij en wetgeving zullen medewerkers continu moeten blijven bijleren en hun werkzaamheden moeten aanpassen. Dit betekent dat ontwikkelen van digitale vaardigheden bij medewerkers ook belangrijk is voor de veiligheid. Het is een blijvend proces van continu veranderen. Naast slimme hulpmiddelen om medewerkers te ondersteunen, vraagt dit om voldoende verandervermogen, bewustwording en kennis bij de medewerkers. Kennis van AVG, het kunnen herkennen van phishing mails of virussen. Of het instellen van een sterk wachtwoord en de computer 'locken' als men even van de plaats gaat. Maar ook kennis hebben van de bedrijfsapplicaties en slimmer leren werken draagt bij aan het verhogen van de digitale vaardig- en veiligheid.

Cyberfeitjes

Menselijke fout

Volgens verschillende onderzoeken en rapporten wordt ongeveer 85% van de cybersecurity-inbreuken veroorzaakt door menselijke fouten. Dit kan bijvoorbeeld komen door onvoldoende beveiliging van wachtwoorden, het openen van verdachte e-mails of bijlagen, of het gebruiken van onveilige netwerken of apparaten.

85%

E-mail is kwetsbaar

Ongeveer 94% van alle malware wordt via e-mail verstuurd. Dit gebeurt vaak via phishing-e-mails, waarbij cybercriminelen zich voordoen als een legitieme afzender en de gebruiker verleiden om op een link te klikken of een bijlage te openen die malware bevat.

94%

Prognose wereldwijde kosten 2025

De jaarlijkse wereldwijde kosten van cybercriminaliteit voor 2025 geschat op $10,5 biljoen. Deze prognoses zijn gebaseerd op de huidige trends en de groei van digitale technologieën en de toenemende aanwezigheid van deze technologieën in verschillende aspecten van ons leven. De kosten van cybercrime kunnen variëren van directe kosten, zoals het betalen van losgeld of het herstellen van systemen na een aanval, tot indirecte kosten, zoals reputatieschade en verlies van vertrouwen in de digitale economie.

10,5 Bln

Nepsites nemen toe

In januari 2021 ontdekte Google meer dan 2,1 miljoen phishingsites. Dit toont aan dat phishing-aanvallen een groot en voortdurend probleem zijn. Naar verwachting neemt het aantal nepsites alleen maar toe.

2,1 Mln

Valse identiteiten doen het goed

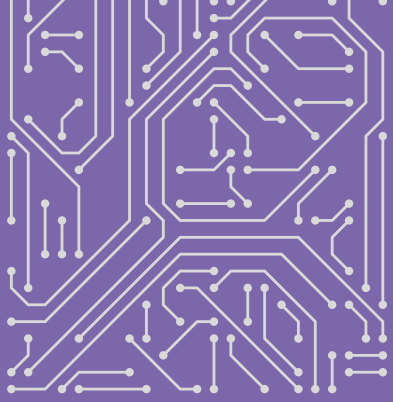
Social engineering tactieken, zoals phishing en pretexting, zijn een van de meest voorkomende manieren waarop cybercriminelen toegang proberen te krijgen tot gegevens en systemen van onderwijsinstellingen. Volgens verschillende onderzoeken gaat meer dan 40% van de cyberbeveiligingsincidenten in het onderwijs om social engineering tactieken. Dit komt omdat onderwijsinstellingen vaak een groot aantal gevoelige gegevens hebben, zoals persoonlijke gegevens van studenten en medewerkers, en omdat cybercriminelen weten dat onderwijsinstellingen vaak minder geld en middelen hebben voor cybersecurity.

40%

Geen haast voor cybercriminelen

Volgens een rapport van Mandiant uit 2020, duurde het gemiddeld 207 dagen om inbreuken in de digitale omgeving te ontdekken. Dit is een lange tijd en geeft cybercriminelen een groot voordeel, omdat ze gedurende die tijd toegang kunnen hebben tot gegevens en systemen. Dit is waarom incident response planning en de implementatie van adequaat beveiligingsmaatregelen zoals EDR (Endpoint Detection and Response) belangrijk zijn, zodat organisaties sneller in staat zijn om inbreuken te detecteren en te reageren.

207 Dagen



kien

Samen ICT *voor onderwijs*

Coöperatie KIEN u.a.
Laan der Verenigde Naties 325
3318 LA Dordrecht
088-6575000
info@kienict.nl