VIER DESKUNDIGEN

Cyberaanvallen in de kinderopvang

Sla je de krant open, dan is de kans groot dat je een artikel tegenkomt over een cyberaanval. Met cybercriminelen die steeds slimmer en sneller te werk gaan, neemt het aantal incidenten jaarlijks toe met bijna 70 procent, wat grote schade met zich mee kan brengen. Denk jij dat jouw organisatie niet interessant is voor hackers? Fout. Ook kinderopvangorganisaties kunnen gemakkelijk ten prooi vallen. |

Marie-Claire van Hessen en Britt Vries

Om jou de juiste informatie en handvatten te geven op dit gebied, ging de Beroepsvereniging Directeuren Kinderopvang (bdKO) in gesprek met drie experts: Xander Koppelmans (mede-eigenaar van het e-learning platform MKB Cybertraining en ervaringsdeskundige), Job Kuijpers (oprichter van verzekerings- en beveiligingsbedrijf Eye Security), Peter van Zijl (business development kinderopvang SDB Groep) en Trudy van Iwaarden-Krist (chief customer officer KidsKonnect).

Automatische aanvallen

'In deze digitale tijd moeten we er samen voor zorgen dat we het cybercriminelen niet te makkelijk maken. We hebben immers te maken met gegevens van medewerkers, ouders én van de kinderen. Het is daarmee cruciaal om van veiligheid een prioriteit te maken. Ik zie het goed inrichten van cybersecurity als een plicht voor alle software aanbieders werkzaam in de kinderopvang', stelt Trudy van Iwaarden-Krist.

Want niemand ontspringt de dans, daar zijn alle vier de experts het over eens. Het is belangrijk dat ook in de kinderopvang de bewustwording wordt vergroot over de risico's en de werkwijze van cybercriminelen. Enkel grote bedrijven halen steeds het nieuws, maar iedereen kan gemakkelijk geraakt worden.

'Denken dat er niets van waarde of geld te halen is en dat een organisatie hiermee niet interessant is voor cybercriminelen is onjuist. Cyberaanvallen gaan automatisch en criminelen weten op voorhand niet wie ze hacken. Pas als ze binnen zijn, kijken ze op welke manier ze de meeste schade kunnen aanrichten', vertelt Xander Koppelmans.

Cybercriminelen verzenden zogenoemde phishing mails op industriële schaal, en naar schatting 30 procent van de ontvangers klikt toch op de link daarin. Daarnaast is software in alle gevallen kwetsbaar, ieder programma bevat wel kleine foutjes die aanvallers ontdekken en waar ze op inspelen. Data bevestigen het: een op de vijf bedrijven in Nederland heeft te maken met een aanval, wat per jaar leidt tot een totale schade van 16 miljard euro.

Zorgplicht bestuurders

De boodschap van de experts is duidelijk. Kinderopvangorganisaties zijn even vatbaar als elk ander bedrijf. En ook zij hebben de plicht om te voldoen aan de AVG-wetgeving over persoonsgegevens. 'Serieus ondernemen vraagt om de benodigde stappen in cybersecurity, dat zien steeds meer bestuurders in. De directie is verantwoordelijk voor alle data van klanten, medewerkers, ouders en de kinderen. Daar hoor je goed voor te zorgen', vat Job Kuijpers samen.

Krijgen cybercriminelen toegang tot je systeem, door bijvoorbeeld een ransomware-aanval uit te voeren, dan wordt er vaak gekozen uit twee opties. De eerste is dat jouw gegevens digitaal 'gegijzeld' worden en jou de toegang wordt ontzegd. De tweede is dat er wordt gedreigd om de data publiek te maken. Beide scenario's kunnen tot ongekende schade leiden.

Door de aanval wordt een stop gezet op alle dagelijkse digitale businessprocessen waarbij gaten in de data de bruikbaarheid van de systemen flink aantasten. 'Zelfs "slechts" twee weken aan verloren gegevens kan als resultaat hebben dat je nog jarenlang te maken hebt met problemen in de administratie, dossiers, planning en facturatie', vertelt Job Kuijpers.

Doemscenario's

Daarnaast kun je last krijgen als gevoelige informatie openbaar wordt gemaakt, denk aan reputatieschade. Het vertrouwen van jouw klanten is immers aangetast. De verloren werkuren, het herstellen van bestanden en kosten voor nieuwe servers en software maken dat de gemiddelde schade per incident gemiddeld 340.000 euro is.

In het ergste geval kan een data-lek zelfs leiden tot identiteitsfraude en afpersing. Xander Koppelmans legt uit hoe de zwarte markt werkt: 'Een cybercrimineel krijgt toegang tot een e-mail en wachtwoord en verkoopt dit door aan een andere hackergroep, die vervolgens kijkt of andere wachtwoorden overeenkomen of er toevallig een kopie van een paspoort of BSN-nummer in staat. Zo wordt het profiel verrijkt en de waarde van de gegevens verhoogd tot de aan te richten schade het grootst is.' Doemscenario's te over dus.

Een eerste stap om cybercriminaliteit in een organisatie te voorkomen is bewustwording. Iedereen die gebruikmaakt van de interne- en externe systemen en programma's moet van de juiste kennis en risico's worden voorzien. Xander Koppelmans vergelijkt het met een digitale snelweg: 'Rijden we zonder rijbewijs op de snelweg, dan ontstaan er veel ongelukken.'

'Dit omdat we ons massaal niet bewust zijn van de gevaarlijke gevolgen. We handelen daar niet naar, omdat we denken dat het ons toch niet gebeurt óf dat het onze verantwoordelijkheid niet is. Hackers lachen zich suf hoe makkelijk het daarom nog is om in te breken. Iedereen in jouw organisatie aan een digitaal rijbewijs helpen is daarom een mooie eerste actie'.

Een tweede stap is om bij de wachtwoorden voor de systemen, programma's en wifi te denken aan de moeilijkheidsgraad, de uniekheid van de wachtwoorden en eventueel de inzet van een wachtwoordmanager. Een simpel wachtwoord van acht karakters is binnen één seconde te hacken. Denk daarbij dus aan de lengte, afwisseling van grote en kleine letters en de toevoeging van nummers en symbolen en kijk naar welke apparaten allemaal op de wifi aangesloten zijn – dat zijn er meer dan je waarschijnlijk denkt.

Two-factor authenticatie wordt hierbij door Koppelmans daarnaast als must gezien. Een laatste simpele tip is om te letten op updates van de programma's. 'Updates worden niet gelanceerd omdat het een nieuwe of betere versie van het product is. Het is niet anders dan dat er een foutje is ontdekt in de software. Als jij hier een melding van krijgt, dan zijn cybercriminelen hier ook van op de hoogte. Wacht hier dus niet mee'.

Peter van Zijl voegt hieraan toe: 'Bepaal intern welke stappen je kunt zetten om het cybercriminelen zo lastig mogelijk te maken, maar werp ook een blik naar buiten. Het is duidelijk dat ieder bedrijf te maken kan krijgen met cyberattacks, en dat geldt eveneens voor de bedrijven achter de operationele systemen die jij als organisatie gebruikt.'

'Denk bijvoorbeeld aan het ouderportaal en de software voor planningen en financiën. Ga daarom altijd in gesprek met de

>

leveranciers over hoe zij je data en de toegankelijkheid van de software ten alle tijden waarborgen, ook wanneer het bij hén misgaat.'

Noodplan maken

Wat als het noodlot toch toeslaat? Ook als het gaat om cybersecurity geldt dat een goede voorbereiding gelijkstaat aan het halve werk. Dit maakt het opstellen van een noodplan voor als het misgaat cruciaal, want ook na een aanval kunnen verkeerde handelingen worden uitgevoerd.
Dat iedereen hun werkzaamheden online moet stoppen is vanzelfsprekend. Maar dat de verbinding van de apparaten moet worden verbroken, maar de apparaten zelf wél aan moeten blijven staan, zal voor velen nieuws zijn. En ook dat je moet denken aan met wie je hebt gecommuniceerd. Een verstuurde e-mail kan bijvoorbeeld een corrupt bestand bevatten waardoor ook anderen in gevaar worden gebracht.
Bel daarnaast direct de it-partner of cyberverzekering en de politie, zij zijn de experts die jou begeleiden in een goede afhandeling. Maak hierbij gebruik van de positieve aspecten van technologie, geeft Xander Koppelmans als tip: op internet zijn diverse vaste formats te vinden voor een noodplan die jouw dringend benodigde reactie een solide basis kunnen bieden.
En, ook niet onbelangrijk: maak een plan voor crisiscommunicatie. Sinds de introductie van AVG hebben organisaties een verplichting om een data-lek binnen 72 uur te melden bij de Autoriteit Persoonsgegevens, daarbij is het verstandig om ook je stakeholders op de hoogte te stellen. Een crisiscommunicatieplan kan jouw reputatieschade minimaliseren.

Ondersteuning

Met veertien jaar ervaring bij de inlichtingen- en veiligheidsdienst heeft Job Kuijpers veel inzicht gekregen in de risicoprofielen op het gebied van cybersecurity. Waar alle bovengenoemde maatregelen en veiligheidsprogramma's, zoals firewalls, het risico en de schade kunnen beperken, is een aanval nooit volledig te voorkomen, stelt hij.
Job: 'Vergelijk het met een brand. Welke maatregelen je ook treft, branden kunnen uitbreken. De impact en schade kun je daarentegen wel verminderen. Dit werkt goed en zo is het ook bij cyberaanvallen. Het klinkt misschien tegen-intuitief, maar genezen is in dit geval beter dan voorkomen.'
Dit maakt het inschakelen van een goede securitypartner van groot belang. Geavanceerde cybersecurity, uitgevoerd door experts, zorgt ervoor dat er direct actie wordt ondernomen wanneer verdacht gedrag zich voordoet en kan zorgen dat de crimineel veelal zonder schade weer uit de systemen wordt gezet.
Job Kuijpers geeft als tip om ook de verzekeringsintermediair in te schakelen om op onafhankelijke wijze naar de juiste partijen te worden verwezen voor advies en implementatie. Partijen die exact kunnen bepalen welke type data de organisatie opslaat, welke beveiliging daarbij hoort en welke stappen gezet moeten worden.
Hij benadrukt het belang van een verzekering en van juridische ondersteuning voor als het wél mis gaat. 'Cyber is net zo als een accountant. Professionele hulp en advies is een must. Gelukkig kennen we in Nederland de beste cyberspecialisten van Europa en staan we in de wereldtop als het gaat om het aanbod in krachtige programma's'.
En een laatste tip van de securityexperts: je kunt het risico dat jouw organisatie loopt op gemakkelijke wijze controleren door na te gaan of je verzekerbaar bent. Wil de verzekering je niet aanraken? Dan ben je er zeker van dat je onvoldoende maatregelen tegen cybercriminaliteit hebt genomen.

Marie-Claire van Hessen en Britt Vries werken bij communicatiebureau MCPR.

'Eén op de vijf bedrijven in Nederland heeft te maken met een aanval, wat per jaar leidt tot een totale schade van 16 miljard euro.'

VERENIGINGSNIEUWS

De bdKO, de beroepsvereniging van directeuren in de kinderopvang, heeft als doel het realiseren en handhaven van een integer, competent en innovatief management in de kinderopvang. De bdKO biedt haar leden een platform voor kennisuitwisseling, een bron van informatie en een netwerk van collega's.

De bdKO onderneemt tal van activiteiten en organiseert diverse bijeenkomsten. Zo organiseert de bdKO twee keer per jaar Landelijke Bijeenkomsten, maar ook trainingen, workshops, intervisie en 'aan tafel met'-bijeenkomsten met politieke woordvoerders kinderopvang. Deskundige professionals zijn verbonden aan de bdKO, die leden advies op maat kunnen geven. Leden hebben continu toegang tot bdKO Kennisdeler waarin alle beschikbare kennis en inzichten gedeeld worden.

Zien we je op één van onze volgende bijeenkomsten?

Ontbijtsessie: toezicht GGD op de kinderopvang – 17 januari 2024

Workshop Crisiscommunicatie en -management – 30 januari 2024

Mediatraining – 30 januari 2024

bdKO Landelijke Buitendag – 20 juni 2024

bdKO Landelijke Dag – 26 september 2024

Zie voor meer informatie over deze en andere bijeenkomsten: www.bdko.nl

Geïnteresseerd in andere bijeenkomsten van de bdKO?

Heb je een aantal interessante bijeenkomsten langs zien komen en heeft dat je interesse gewekt, maar ben je nog geen lid van de bdKO? Wij nodigen je uit om deel te nemen aan een van onze evenementen of webinars. Zo kun jij vrijblijvend kennismaken met onze beroepsvereniging. Neem een kijkje op onze website www.bdko.nl voor de komende bijeenkomsten en meld je aan met één belletje naar (079) 363 81 02.

Lid worden?

Wil je graag de voordelen ontdekken van lidmaatschap van de bdKO? In het eerste jaar krijg je 50 procent korting op de deelnamekosten van onze bijeenkomsten. Zo kun jij op een laagdrempelige wijze beoordelen of onze beroepsvereniging iets voor je is.