procurios

Zo houd je de gegevens en systemen van je vereniging veilig

CYBERSECURITY

7 low budget maatregelen voor een betere cybersecurity die iedere vereniging kan toepassen

Steeds vaker lezen en horen we over cyberaanvallen in onze maatschappij. Niet alleen bedrijven zijn het slachtoffer, ook verenigingen lopen risico. Vooral persoonlijke gegevens zijn in trek bij cybercriminelen. Dat zijn natuurlijk data die verenigingen bij uitstek hebben over hun leden. Het is daarom geen overbodige luxe om eens goed te kijken naar hoe jouw vereniging deze gegevens beschermt.

Denk eens na over alle gegevens die een vereniging verzamelt en bewaart van leden. Wanneer deze data in verkeerde handen vallen, zou een cybercrimineel direct toegang hebben tot volledige namen, adressen, betalingsgegevens en nog veel meer. Deze informatie wordt door cybercriminelen graag buitgemaakt, omdat ze veel geld waard zijn op het dark web, het gedeelte van internet dat vrijwel geen toezicht kent en daarom veel gebruikt wordt door criminelen.

Persoonlijke gegevens worden daar verhandeld om bijvoorbeeld valse paspoorten te maken of een complete identiteit te stelen. Iedere keer dat er een datalek plaatsvindt, zijn er duizenden, wellicht miljoenen mensen bereid om voor deze gelekte informatie te betalen.

Niet alleen zou het forse reputatieschade opleveren wanneer de gegevens van leden buitgemaakt worden, de leden zelf lopen dan ook risico op identiteitsdiefstal. En wat te denken van de continuïteit van de vereniging? Wanneer er een cyberaanval plaatsvindt, hoe lang duurt het dan voordat alle systemen weer up and running zijn en medewerkers weer aan de slag kunnen?

Inhoudsopgave

Sluit ramen en deuren

De vraag is niet langer of een vereniging ooit het slachtoffer wordt van cybercrime, maar eerder wanneer.

Toch staat het onderwerp cybersecurity lang niet bij iedere vereniging hoog op de agenda. Dat komt vaak door de overtuiging dat kleine organisaties niet interessant zijn voor cybercriminelen. Daarnaast wordt de waarde van de gegevens die een vereniging bezit vaak onderschat. Helaas zijn beide overtuigingen niet waar. Juist de persoonlijke data waarover een vereniging beschikt, is zeer interessant voor criminelen. Daarbij richten ze aanvallen vaak niet specifiek op een organisatie, maar schieten ze met hagel om te zien waar de achterdeur in systemen openstaat.

Cybercriminelen zijn heel pragmatisch. Wanneer de voordeur van jouw vereniging goed op slot is, zullen ze hun geluk eerder bij de buren beproeven. Maar wanneer er naast de voordeur toevallig een keukenraam wagenwijd openstaat, zullen ze het niet laten om naar binnen te gaan.

Niet alleen cybercriminelen vormen een risico, het grootste gevaar loert binnen de vereniging. Slechts de helft van de datalekken in kleine organisaties is te wijten aan kwaadwillende hackers. De andere helft is het gevolg van onjuiste opslag en verwerking van gevoelige gegevens door medewerkers en vrijwilligers.

Niet iedere vereniging heeft de kennis of het budget om forse securitymaatregelen rond de systemen te bouwen. Gelukkig is dat ook helemaal niet nodig. Met een aantal effectieve maatregelen kun je zonder uitgebreide kennis of torenhoge budgetten zorgen dat de privacygevoelige data in je vereniging veilig is en blijft.

Cyberaanvallen op verenigingen uit de praktijk

Phishing bij het Interprovinciaal Overleg

Het Interprovinciaal Overleg (IPO) werd in 2019 slachtoffer van een hack doordat een medewerker een phishingmail opende. Het IPO is een vereniging die de belangen van de 12 Nederlandse provincies behartigt in Den Haag. De medewerker die op de phishinglink klikte werd gevraagd de inloggegevens voor zijn e-mailaccount in te vullen. Dat deed hij, waarna de cybercriminelen toegang hadden tot zijn e-mailbox en hij niet meer. Vervolgens verstuurden de cybercriminelen uit zijn naam e-mails naar contacten. Het is niet helder wat het doel van deze berichten was. Toen de medewerker zich realiseerde wat er aan de hand was, zijn de nodige maatregelen genomen om de cybercriminelen uit te sluiten van het systeem en zijn de contacten op de hoogte gebracht.

Dit incident lijkt, afgaande op de berichtgeving in de media, met een sisser te zijn afgelopen. Het IPO bleek zijn medewerkers niet te trainen op het herkennen van phishingmails.

Nationale Vereniging De Zonnebloem slachtoffer van ransomware

In 2017 werd Nationale Vereniging De Zonnebloem slachtoffer van ransomware. De bestanden op de systemen van de vereniging werden versleuteld en er werd losgeld geëist om weer toegang te krijgen. In het geval van De Zonnebloem ging het om 4700 aanmeldformulieren van mensen die meegingen op de vakanties die de vereniging organiseert. De formulieren bevatten zowel gewone als bijzondere persoonsgegevens, bijvoorbeeld over de lichamelijke gesteldheid van de deelnemers. Daarmee was het dus een kwalitatief datalek.

Gelukkig bleven de gevolgen van de ransomware-aanval voor De Zonnebloem beperkt, omdat er geen persoonsgegevens gestolen waren. Het losgeld hoefde niet te worden betaald, omdat de vereniging beschikte over een goede back-up van het bestand.

1 Maak iemand verantwoordelijk voor cybersecurity

Niet alleen wil je als vereniging liever geen slachtoffer worden van een cyberaanval, je moet bovendien voldoen aan de Algemene verordening gegevensbescherming (AVG), de privacywetgeving die sinds 2018 in de hele EU van kracht is.

De AVG gaat over het rechtmatig omgaan met persoonsgegevens. Sinds de invoering van deze wet hebben mensen meer rechten en mogelijkheden gekregen op het gebied van privacy. Organisaties hebben hierdoor meer verantwoordelijkheden en de toezichthouder Autoriteit Persoonsgegevens (AP) heeft onder de AVG meer bevoegdheden gekregen. Wanneer er onverhoopt persoonlijke gegevens van je leden op straat komen te liggen en je niet kunt aantonen dat je voldoende maatregelen hebt genomen om dit te voorkomen, loop je kans op een forse boete van de AP.

Door een privacy/security verantwoordelijke aan te wijzen binnen de vereniging, kun je beter borgen dat maatregelen worden ingesteld, gemonitord en nageleefd. Wanneer je security een verantwoordelijkheid maakt van iedereen binnen de vereniging, is de kans groot dat niemand zich verantwoordelijk voelt. Deze verantwoordelijke hoeft geen ICT'er of techneut te zijn, maar moet wel over het mandaat beschikken om externe expertise in te schakelen op het moment dat dit noodzakelijk wordt geacht.

Wat heb ik eraan?

De persoon die verantwoordelijk is voor cybersecurity binnen je vereniging, kan erop toezien dat de AVG wordt nageleefd, maar kan ook gesprekken over security voeren met bijvoorbeeld leveranciers en bureaumedewerkers. Het gevaar op een datalek of cyberincident komt namelijk niet altijd van buiten, maar vaker van binnen een organisatie. De security-verantwoordelijke kan ervoor zorgen dat medewerkers worden getraind in het herkennen van cybercriminaliteit en in het juist en veilig handelen wanneer ze met privacygevoelige gegevens werken.

Dit is ook de persoon die het overzicht heeft en bewaart. Die weet waar de risico's liggen en ervoor kan zorgen dat deze worden afgedekt. Richting leden en bestuur kan deze verantwoordelijke inzichtelijk maken hoe de vereniging omgaat met cybersecurity. Dat zorgt niet alleen voor betrouwbaarheid, maar straalt ook af op het imago van de vereniging.

Hoe moet ik het doen?

Degene die verantwoordelijk wordt gemaakt voor cybersecurity hoeft niet perse technische kennis te hebben. Het is wel zaak dat deze persoon structuur kan aanbrengen, zaken kan uitbesteden, overzicht kan bewaren en weet waar de benodigde informatie en kennis vandaan gehaald kan worden.

2 Maak periodiek een risicoanalyse

De eerste stap naar een veiligere vereniging is het weten welke waardevolle informatie je bezit, waar die zich bevindt in de vereniging en welke risico's deze data lopen.

Breng in kaart welke systemen onmisbaar zijn voor de dagelijkse operatie van de vereniging. Welke data is kritisch? Zorg dat je ook helder hebt welke mensen toegang hebben tot welke systemen. Is het noodzakelijk dat iedereen bij alle gegevens in het CRM-systeem kan of is dit voorbehouden aan een selecte groep medewerkers? Zijn de mensen die met persoonlijke gegevens van leden werken, zich bewust van mogelijke cybergevaren en de werkwijze van cybercriminelen?

Ga ook in gesprek met de leveranciers van je IT-systemen en bespreek wat zij doen om de integriteit van de data te waarborgen. Maakt de leverancier van jouw clouddienst bijvoorbeeld regelmatig back-ups? En hoe beschermt hij zijn systemen tegen DDoS-aanvallen of hacks?

Wat heb ik eraan?

Het is belangrijk om dit niet eenmalig te doen, maar periodiek.

Niet alleen veranderen processen, medewerkers en gegevens, maar zeker ook de dreiging van buitenaf. Het identificeren van potentiële bedreigingen en de inspanningen om beveiligingsincidenten te beperken, bespaart de vereniging op lange termijn geld. De eerste keer dat zo'n risicoanalyse wordt uitgevoerd, zal het meer tijd en inspanning kosten.

Door het de eerste keer goed te doen, creëer je een herhaalbaar proces dat door anderen kan worden opgepakt in het geval van vertrekkende medewerkers. En, wanneer je weet waar de zwakke punten van je vereniging liggen, krijg je een beter idee van de gebieden waarin de organisatie moet groeien en waarin ze wellicht moet investeren. Een goede risicoanalyse helpt inbreuken en andere beveiligingsincidenten te voorkomen, doordat het de security van de vereniging helpt verbeteren. Hierdoor blijven de gevolgen van aanvallen en inbreuken op persoonlijke gegevens beperkt.

Hoe moet ik het doen?

Er is een aantal partijen die een gratis cyber-scan aanbiedt, zoals het cybersecuritybedrijf EYE Security, maar ook verzekeraar Nationale Nederlanden en de KvK. Zo'n scan biedt op technisch gebied inzicht in de mogelijke kwetsbaarheden in de systemen van de vereniging. De scans zijn vaak gericht op bedrijven, maar bieden ook inzicht in de veiligheid van het netwerk van een vereniging. Het is raadzaam om eens zo'n scan uit te voeren. Als je weet hoe en waar cyberaanvallen het systeem en processen kunnen binnendringen, kun je beter begrijpen hoe je een potentiële bedreiging kunt herkennen voordat het een groot probleem wordt.

Vervolgens breng je het hele IT-landschap van de vereniging in kaart. Documenteer elk apparaat, waaronder computers, tablets, routers, printers, servers en telefoons, in het netwerk. Leg vervolgens vast hoe deze bronnen worden gebruikt en hoe ze met elkaar verbonden zijn.

Maak een lijst van gegevenstypen, afdelingen die toegang hebben tot systemen en leveranciers die in aanraking komen met netwerkbronnen en -informatie. Noteer hoe informatie en gegevens zich door het netwerk bewegen en met welke componenten ze onderweg in aanraking komen.

Breng daarna de prioriteiten van de risico's in kaart. Hoe zou een cyberaanval de vereniging bijvoorbeeld schaden? Welke informatie loopt het meeste risico? Maak een lijst van alle potentiële risico's en rangschik ze op een schaal van laag, gemiddeld en hoog risico. Deze prioriteiten helpen bij het bepalen welke securitymaatregelen er noodzakelijk zijn. Voor het bepalen van een risico wordt meestal gekeken naar de (financiële) schade die een cyberaanval zou aanrichten wanneer informatie gecompromitteerd zou worden.

3 Zorg dat alle systemen up-to-date zijn

Het bouwen van systemen en software is nog altijd mensenwerk. Dat wil zeggen dat er hier en daar onverhoopt een foutje in kan sluipen. Dat hoeft niet altijd erg te zijn, maar wanneer zo'n foutje ervoor zorgt dat er cybercriminelen ongezien toegang hebben tot jouw systemen, wordt het een ander verhaal.

Daarbij werk je vaak met verschillende systemen, denk aan een HR-systeem, een financieel systeem, een CRM en misschien nog een planningsysteem. Die systemen kunnen afkomstig zijn van verschillende leveranciers, maar moeten wel samenwerken met elkaar. Dat punt waarop ze elkaar als het ware aanraken, kan ook kwetsbaarheden bevatten. Je kunt bij regen wel een tunneltje bouwen van de ene tent naar de andere, maar dat wil niet zeggen dat je compleet droog blijft, omdat de tunnel misschien niet volledig aansluit op de opening.

Leveranciers zijn continu bezig om hun software en systemen te verbeteren. Niet alleen door de foutjes die er wellicht ingeslopen zijn te herstellen, maar ook door het leveren van verbeterde functionaliteit en veiligheid. Daarom is het belangrijk dat je alle updates en patches die je krijgt, direct installeert. Op alle systemen waar die software draait.

De meeste cyberaanvallen met een grote impact hebben vaak één ding gemeen: ze zijn gericht op bekende kwetsbaarheden in systemen en software van derden. WannaCry en de hack bij IT-dienstverlener Kaseya zijn spraakmakende voorbeelden van succesvolle aanvallen op ongepatchte systemen.

Maar deze gevallen hebben ook iets anders gemeen: ze hadden allemaal voorkomen kunnen worden. Software-updates en patches werden uitgebracht voordat de aanvallen plaatsvonden, en de enige reden dat zoveel bedrijven het slachtoffer werden van deze cyberaanvallen is dat ze verzuimden deze te downloaden, uit te voeren en te installeren.

Wat heb ik eraan?

Door patches en updates direct te installeren, zorg je dat je je systemen veilig houdt. Je sluit als het ware een deur die op een kier was komen te staan. Cybercriminelen zijn – zoals eerder gezegd – zeer pragmatisch. Het liefst behalen ze grootste resultaten met zo min mogelijk moeite. Dat betekent dat wanneer er een kwetsbaarheid in software bekend wordt, ze daar direct gebruik van maken. De leverancier van die software heeft zijn gebruikers allang een update gestuurd, maar veel organisaties voeren die niet direct uit, wat hen kwetsbaar maakt. Cybercriminelen weten dat. Ze hoeven op deze manier niet zelf te achterhalen waar mogelijke lekken in de software zitten, die krijgen ze op een presenteerblaadje aangeleverd. En omdat veel organisaties van updaten geen prioriteit maken, kunnen cybercriminelen vervolgens eenvoudig in systemen inbreken.

Daarnaast bevatten updates, zoals gezegd, ook nieuwe mogelijkheden of worden zaken vereenvoudigd. Updates zijn altijd een verbetering van de software. En je wilt als vereniging natuurlijk alleen het beste.

Hoe moet ik het doen?

Zodra je een bericht krijgt van je leverancier, of in de software de mogelijkheid krijgt om te updaten, zorg je dat je dit zo snel mogelijk uitvoert. Twijfel je over de authenticiteit van het bericht? Bel dan even met de leverancier van de software. Die kan je ook helpen bij het uitvoeren van de update. Bovendien zorgen veel leveranciers van clouddiensten er automatisch voor dat updates en patches worden uitgevoerd. Zo weet je zeker dat jouw software altijd veilig is.

4 Stel meerfactorauthenticatie (MFA) in

Veel organisaties dwingen hun medewerkers regelmatig hun wachtwoord te wijzigen. Helaas is dat geen garantie voor de veiligheid van je systemen. Sterker nog, het kan juiste verkeerd gedrag uitlokken. Mensen vinden het moeilijk vinden om wachtwoorden te onthouden, en kiezen daarom bijna overal hetzelfde wachtwoord, of wijzigen steeds slechts één of twee karakters. Bovendien gebruiken de meeste mensen een hoofdletter aan het begin van hun wachtwoord en wordt er als speciaal teken vaak een uitroepteken gekozen die het wachtwoord afsluit. Deze voorspelbaarheid en de menselijkheid van medewerkers moet meegenomen worden in het wachtwoordbeleid van de vereniging.

Nóg slimmer is het om multifactorauthenticatie (MFA) te gebruiken. Dat wordt ook wel twee-factor authenticatie of tweestapsverificatie genoemd en is een extra beveiligingslaag die wordt gebruikt om ervoor te zorgen dat alleen bevoegde gebruikers toegang krijgen tot een account. Bij MFA logt een gebruiker in eerste instantie in met zijn gebruikersnaam en wachtwoord (iets dat hij wéét). Maar in plaats van onmiddellijk toegang te krijgen, moet hij nog wat extra informatie (de tweede factor) geven. Dat kan iets zijn dat hij héeft (bijvoorbeeld een telefoon waarop per sms een code binnenkomt) of iets dat hij ís (bijvoorbeeld je vingerafdruk of gezichtsherkenning). Het voordeel van die extra stap is dat wanneer je wachtwoord wordt gestolen of je telefoon kwijt raakt, de kans klein is dat iemand anders toegang heeft tot béide inlogfactoren.

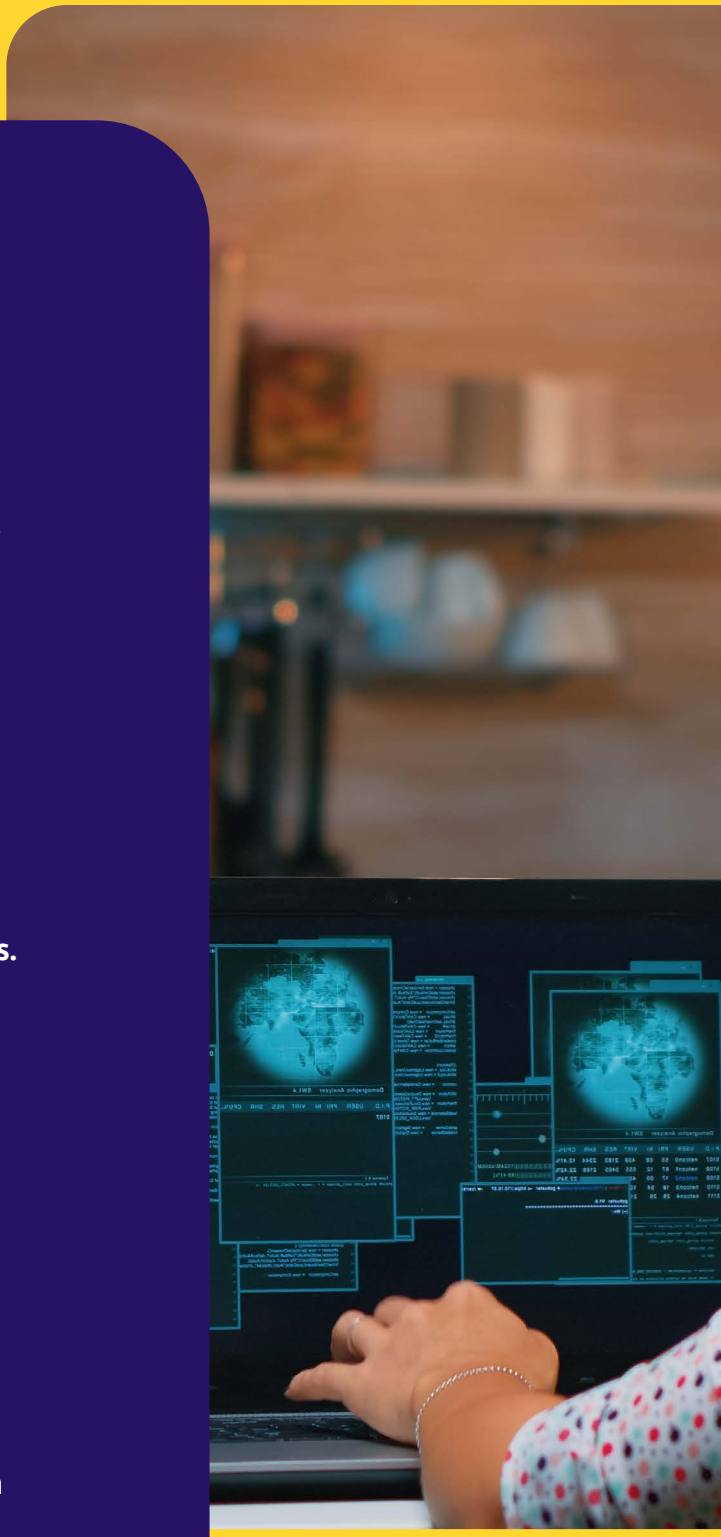
Om het gemak van veilig inloggen te vergroten, kun je als organisatie ook kiezen voor 'Single Sign-on'. Dat betekent dat een gebruiker maar één keer hoeft in te loggen, omdat zijn andere accounts zijn gelinkt met bijvoorbeeld zijn inloggegevens voor Office 365. Wanneer je andere applicaties aan Office 365 koppelt, kun je het zo regelen dat het inloggen op die programma's automatisch op de achtergrond gebeurt, zonder dat de gebruiker dat zelf doorheeft. Zo voorkom je dat iedereen overal accounts heeft met hetzelfde wachtwoord, centraliseer je het inloggen op één plek waar je goede controle over hebt en kun je eisen stellen aan het inloggen.

Wat heb ik eraan?

Voor cybercriminelen is het op dit moment significant moeilijker om in te breken op netwerken waarop gebruikers met MFA inloggen dan op netwerken waar gebruikers zich aanmelden met alleen een wachtwoord. Zeker wanneer je als vereniging nog niet zo ver bent met het trainen van je medewerkers in hun bewustwording van cybercrime, is dit een mooie extra stap die je ervan verzekert dat kwaadwillenden met een wachtwoord niet zo eenvoudig toegang krijgen.

De nieuwste trend op dit gebied is wachtwoordloos inloggen, waarbij feitelijk alleen die tweede stap wordt gebruikt om toegang te krijgen tot systemen en gegevens.

Want aanvallers zijn inmiddels vrij bedreven in het afhandig maken van wachtwoorden van gebruikers. Sterker nog, het lukt ze vaak ook om bijvoorbeeld de cijfercode bij een meerfactorauthenticatie te bemachtigen. Het voordeel van wachtwoordloos inloggen is dat het heel moeilijk is voor een aanvaller om bijvoorbeeld jouw vingerafdruk te verkrijgen. Dat maakt het op dit moment de meest veilige manier om in te loggen. Het voordeel is bovendien dat gebruikers geen wachtwoorden hoeven te onthouden en geen extra stap hoeven uit te voeren om ergens te kunnen inloggen.



Hoe moet ik het doen?

Het is belangrijk om te bepalen welk authenticatiemechanisme je wilt gebruiken. Er is een aantal manieren om gebruikers te identificeren en authenticeren, bijvoorbeeld de gezichtsscan, de vingerafdruk of authenticatie apps. Je wilt het liefst één manier introduceren in je organisatie, zodat de manier van inloggen niet gefragmenteerd raakt en je weer allerlei verschillende systemen moet onderhouden en monitoren.

Vervolgens is het belangrijk om aan bureaumedewerkers uit te leggen waarom je MFA invoert en wat dit van hen vergt. Mocht je op termijn wachtwoordloos willen gaan werken, dan kunnen ze met MFA alvast wennen aan de nieuwe manier van inloggen. Op termijn kun je dan het wachtwoord loslaten en dat zal alleen maar meer gemak en eenvoud brengen voor de medewerkers.

5 Maak regelmatig back-ups en test ze

In de voorbeelden zagen we al dat Nationale Vereniging en De Zonnebloem relatief weinig last had van de ransomware-aanval die hen trof, omdat ze de beschikking hadden over een back-up. Zo'n back-up kan de redding betekenen van de vereniging wanneer alle bestanden versleuteld zijn en er een torenhoge losgeldeis op tafel ligt.

Het maken van back-ups is dus van cruciaal belang voor gegevensbescherming. Een regelmatige gegevensback-up behoedt belangrijke systemen voor gegevensverlies als gevolg van systeemcrashes, malware-infecties, beschadiging en uitval van de harde schijf, enzovoort. Belangrijk hierbij is dat de back-up recent is gemaakt. Hoe groter de periode tussen de back-up en het actuele systeem op het moment van een incident, hoe meer gegevens verloren gaan. Het is daarom raadzaam om dagelijks of wekelijks een back-up te maken.

Experts adviseren om een back-up te maken volgens het 3-2-1-principe. Dat wil zeggen dat je drie back-ups maakt op twee verschillende typen media waarvan er één extern – dus los van het netwerk – wordt bewaard.

Een ander advies is om de gemaakte back-ups regelmatig te testen. Er is niets zo vervelend om te vertrouwen op back-ups om er vervolgens op een cruciaal moment achter te komen dat ze niet functioneren.

Mocht je samenwerken met cloudleveranciers, maak dan met hen afspraken over back-ups en mogelijke data recovery.

Wat heb ik eraan?

Een back-up is een kopie van belangrijke gegevens die wordt opgeslagen op een alternatieve locatie, zodat ze kunnen worden hersteld als ze worden gewist of beschadigd raken. Het biedt de zekerheid van continuïteit in het geval van een incident. Dat hoeft niet altijd een cyberaanval te zijn. Een computer kan op elk moment stoppen met werken, en gegevens op een harde schijf kunnen beschadigd raken of verloren gaan als de harde schijf defect raakt.

Met een back-up ben je ervan verzekerd dat je een bepaald moment in het verleden kunt terughalen en vanaf daar verder kunt werken.

Hoe moet ik het doen?

Er zijn verschillende manieren om een back-up te maken. Je leverancier kan je hierin adviseren.

Het is belangrijk om na te denken hoe je je back-upbeleid wilt inrichten, welke media je gaat gebruiken, hoe vaak je een back-up gaat maken en welke afspraken er zijn met cloudleveranciers.

6 Train je medewerkers

De medewerkers van de vereniging zijn een belangrijke verdedigingslinie voor de organisatie als het gaat om cyberincidenten. Het is daarom belangrijk dat zij getraind worden om mogelijke aanvallen te herkennen en daar op de juiste manier op te reageren. Uit verschillende onderzoeken blijkt dat medewerkers graag veilig willen werken, maar niet altijd weten hoe ze dat moeten doen.

Cybercriminelen proberen op allerlei gewiekste manieren bij organisaties binnen te komen. Daarvoor misbruiken ze bijvoorbeeld het vertrouwen van de verenigingsmedewerkers in andere mensen. Door hen bewust te maken van hoe cybercriminelen werken, kunnen zij alerter reageren op onverwachte vragen of vreemde verzoeken, hoe legitiem ze ook lijken.

Veelgebruikte methodes zijn phishing, social engineering en CEO-fraude. Deze methodes hebben met elkaar gemeen dat ze een bepaalde urgentie oproepen en een actie van de ontvanger vereisen. Toch zijn de nepmails vaak wel te herkennen, hoewel dat niet altijd eenvoudig is. Leer medewerkers wat cybercrime is, wat ze kunnen doen om veilig te werken en hoe ze de signalen kunnen herkennen.

Enkele rode vlaggen in e-mails die wijzen op phishing zijn bijvoorbeeld:

- **Grammaticale en spelfouten**
- **Onduidelijke of onbekende afzender**
- **Een aanbod, vraag of instructie die argwaan wekt**
- **Links die naar dubieuze websites verwijzen**

Maak het voor medewerkers eenvoudig om verdachte berichten te melden en zorg dat er geen persoonlijke consequenties zijn wanneer iemand onverhoopt toch op een nepmail klikt. Wanneer verenigingsmedewerkers zich veilig voelen om afwijkingen te melden, zullen ze graag bereid zijn om bij te dragen aan de security van de verenigingsinformatie.

Wat heb ik eraan?

Het trainen van je medewerkers, je belangrijkste verdedigingslinie, zorgt ervoor dat cybercriminelen minder makkelijk toegang kunnen krijgen tot je systemen. Herinner je je het pragmatisme van de criminelen? Wanneer jouw deur dicht zit, proberen ze het liever bij de buren, waar de boel wagenwijd open staat.

Hoe meer de medewerkers alert zijn op mogelijke cybercrime, hoe minder snel ze erin tuinen. Wanneer ze weten welke bedreigingen er zijn, hoe ze die kunnen herkennen en waar ze die vervolgens moeten melden, is het voor cybercriminelen veel moeilijker om waardevolle data buit te maken. Het draagt dus enorm bij aan de veiligheid van de vereniging.

Hoe moet ik het doen?

Er zijn talloze 'awareness' programma's beschikbaar die je kant-en-klaar kunt afnemen bij een leverancier. Maar wanneer daar kennis en gelegenheid voor is, kan ook de security-verantwoordelijke binnen de vereniging tekst en uitleg geven aan medewerkers. Dit kan in de vorm van een workshop, maar ook door middel van een mailing.

Het is belangrijk om je te realiseren dat deze awareness trainingen niet eenmalig zijn, maar dat de informatie en kennis op regelmatige basis gedeeld moeten worden, omdat het anders wegzakt bij de medewerkers.

Het is ook raadzaam om af en toe phishing simulaties uit te voeren om zo te kunnen bepalen of de trainingen ook daadwerkelijk meer kennis en alertheid bij medewerkers opleveren er zijn met cloudleveranciers.

7 Stel een stappenplan op voor incidenten

Natuurlijk doe je al het mogelijke om je vereniging veilig te houden, maar cybercrime is inmiddels een professionele bedrijfstak geworden waar vele miljarden in omgaan. Het vechten tegen cybercriminelen is een kat-en-muisspel.

De kans dat een vereniging wordt getroffen door een hack, een datalek of ander cyberincident is levensgroot. Het is verstandig om vooraf na te denken hoe te handelen in zo'n geval.

Een draaiboek voor het geval een organisatie wordt getroffen door een cyberincident, noemen we een incident response plan. Het beschrijft het proces van hoe de vereniging omgaat met het incident zelf en de gevolgen ervan.

Een incident response plan kan worden omschreven als een set instructies om medewerkers te helpen om beveiligingsincidenten te detecteren, hierop te reageren en mogelijke schade te herstellen. Het doel is om snel, kalm en adequaat te kunnen reageren om schade te beperken en herstelwerkzaamheden te minimaliseren.

Wat heb ik eraan?

Doordat er op een rustig moment wordt nagedacht over hoe te handelen bij een incident, is een vereniging beter in staat heldere beslissingen te nemen dan wanneer er in de paniek van het moment moet worden gehandeld. Ook kan voorkomen worden dat er cruciale onderdelen worden vergeten in de hectiek.

Bovendien voelt je je minder overvallen door het incident, en kun je dus adequater handelen, wanneer je weet hoe je moet handelen, omdat je daar vooraf over hebt nagedacht. Een incident response plan bevat niet alleen acties en adviezen over het incident zelf, maar ook daarna. Zijn er bijvoorbeeld persoonsgegevens verloren? Dan is het zaak om dat binnen 72 uur aan de AP te melden. Heb je dat niet in een overzichtelijk plan staan, dan is de kans dat je zo druk bent met het oplossen van het incident dat je uiteindelijk te laat bent met je melding, mogelijk met vervelende gevolgen.

Een incident response plan geeft je houvast, structuur en overzicht in het geval van een incident. Daardoor kun je waarschijnlijk de schade beter beperken dan wanneer je ter plekke moet bedenken welke acties noodzakelijk zijn.

Hoe moet ik het doen?

Er is veel informatie te vinden over hoe je een incident response plan moet opstellen. Je IT-leverancier kan je hier ook bij helpen. Maar kijk bijvoorbeeld ook eens bij het Digital Trust Center van de Rijksoverheid. Zij hebben een helder overzicht gemaakt voor wat te doen bij een cyberincident.

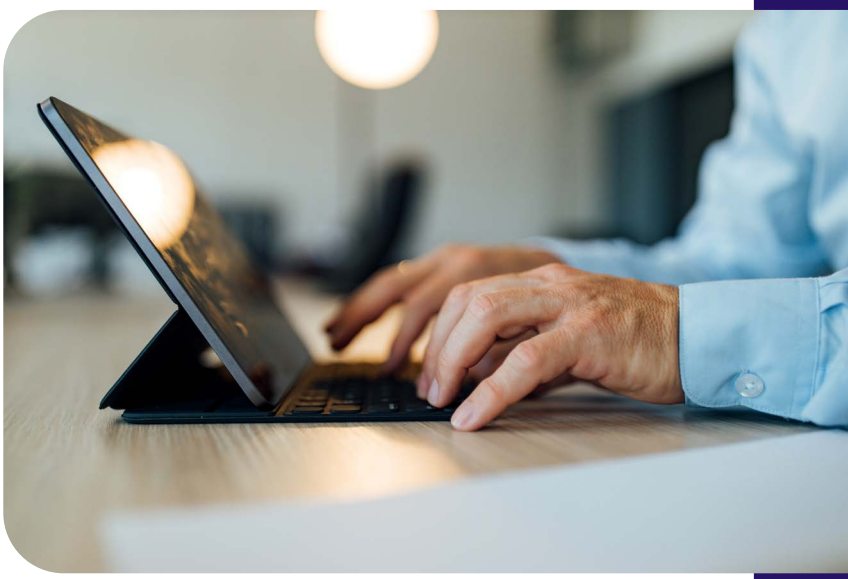
Een incident response plan bevat een aantal elementen en je kunt het zo uitgebreid maken als je zelf wilt. In elk geval staat erin hoe mogelijke incidenten gedetecteerd worden en waar die moeten worden gerapporteerd. Er wordt beschreven hoe het incident wordt geanalyseerd, ingeperkt en geneutraliseerd. Ook zou erin moeten staan welke zaken na het incident moeten worden opgepakt, zoals bijvoorbeeld communicatie naar de leden.

Geen tijd om achterover te leunen

Cybersecurity is een van de belangrijkste onderwerpen in onze maatschappij op dit moment. De wereld digitaliseert steeds verder en het is belangrijk dat we ook digitaal veilig zijn en blijven. Er rust een grote verantwoordelijkheid op verenigingen om op een goede manier met de persoonlijke gegevens van leden om te gaan.

Online is er ontzettend veel informatie te vinden over cybersecurity. Zoveel dat het soms lastig is om tussen de bomen door het bos nog te zien. Wanneer je meer wilt weten, kun je vaak gratis en vrijblijvend met een securityorganisatie praten, zeker naar aanleiding van een gratis scan.

We laten je achter met een laatste tip. Wil je weten of de e-mailadressen van jouw vereniging ooit in een gehackte database zijn voorgekomen? Kijk dan eens op **'Have I Been Pwned'.** Dat is een website waarop internetgebruikers kunnen nagaan of hun persoonsgegevens door datalekken zijn gecompromitteerd. De dienst verzamelt en analyseert honderden databasedumps met informatie over miljarden gelekte accounts, en stelt gebruikers in staat naar hun eigen informatie te zoeken door hun gebruikersnaam of e-mailadres in te voeren.

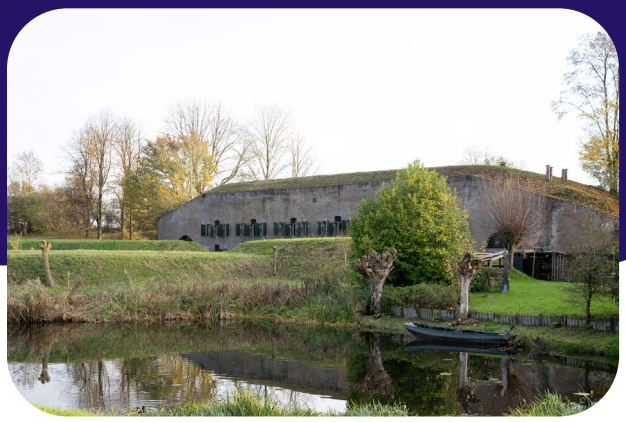


Een totaaloplossing voor verenigingen en goede doelen

Wij helpen organisaties met een maatschappelijk doel een krachtige en duurzame relatie met hun doelgroepen vorm te geven. Dat is onze missie en we zetten ons iedere dag in om onze klanten te helpen hún missie te realiseren. Dat doen we met ruim 40 Procurioten in Nederland en België. We gaan daarbij voor impact, groot of klein, en voor een prettiger wereld, ook als de invulling daarvan voor iedereen net iets anders is.

Wij vinden dat aandacht voor wat er echt toe doet in de wereld, schaars is. Betekenisvolle verbindingen zijn daarom essentieel. Verenigingen, goede doelen, stichtingen en andere non-profits zijn als geen ander in staat die te creëren. Ons open online softwareplatform geeft hen de middelen om het verschil te maken. Zo helpen wij met onze kennis en technologie om de impact van organisaties met een maatschappelijke missie iedere dag te laten groeien.

Misschien heb je vragen naar aanleiding van deze gids en wil je meer weten. Of misschien heb je een ander vraagstuk. Geef ons gerust een belletje, **stuur ons een e-mail met je vraag of verzoek** of **plan een demo**: we helpen je graag verder, of op weg.



Kantoor België
Hendrik Consciencestraat 5 / bus 302
2800 Mechelen
+32 3 237 41 45 (BE)
info@procurios.be
www.procurios.com

Kantoor Nederland
Fortweg 9
3992 LX Houten
+31 343 59 60 40 (NL)
info@procurios.nl
www.procurios.com