Stappenplan Cyberveiligheid in culturele organisaties.

Hoe zorg je ervoor als culturele organisatie dat je digitaal veilig en toekomstbestendig bent. Dit vraagstuk is actueler dan ooit! Culturele organisaties gebruiken steeds vaker (externe) digitale systemen in hun dagelijkse processen, bijvoorbeeld voor ticketing, ICT-ondersteuning of voor het beheer van kunst-collecties, met alle risico's van dien. Door dit stappenplan te doorlopen, vergroot je niet alleen het bewustzijn rondom digitale veiligheid, maar werk je ook actief aan een robuuster beveiligingsniveau. Het is gericht op medewerkers die verantwoordelijk zijn voor ICT en/of de beveiliging van hun organisatie.

DEN

Stap 1

Weet wat je moet beschermen: jouw kroonjuwelen

Iedere organisatie, groot of klein, heeft informatie of processen die van cruciaal belang zijn voor het succes en de bedrijfscontinuïteit: dit zijn jouw kroonjuwelen. Denk niet alleen aan digitale gegevens of applicaties, maar ook aan fysieke documenten en kennis die in hoofden van medewerkers zit. Voorbeelden van kroonjuwelen zijn je digitale collectie, het ticketingsysteem en systemen waar persoonsgegevens in staan, maar ook de klimaatbeheersing van tentoonstellingsruimtes. Bedenk hierbij: uitval is uitval. Of dat nu komt door een hack of door een stroomstoring.

Het identificeren van jouw kroonjuwelen is de eerste stap naar effectieve informatiebeveiliging. Vraag jezelf af:

- **Welke informatie of systemen zijn essentieel voor onze dagelijkse activiteiten?**
  Denk aan een ticketingsysteem dat bezoekers toegang geeft of een database met donateursgegevens.
- **Wat zou een grote impact hebben op onze organisatie als het verloren gaat of toegankelijk wordt voor onbevoegden?**
  Je kunt hierbij denken aan een kunstcollectie die digitaal wordt opgeslagen of plannen voor een exclusieve expositie.
- **Wie zou wakker liggen als deze informatie op straat komt te liggen?**
  Bijvoorbeeld als financiële gegevens van sponsoren worden gelekt of restauratieplannen worden gesaboteerd.

Door deze vragen te beantwoorden, kun je prioriteiten stellen. Richt je als eerste op de processen en informatie die essentieel zijn voor jouw organisatie.

Het kan goed misgaan als je geen zicht (meer) hebt op je kroonjuwelen. Bij cyberincidenten kunnen de consequenties namelijk enorm zijn. Daarnaast is op sommige kroonjuwelen mogelijk wetgeving van toepassing en krijg je een boetes opgelegd omdat je niet voldoet aan de AVG-wetgeving.

Hieronder staan een aantal voorbeelden van consequenties nadat het zicht op kroonjuwelen is verdwenen:

1. Persoonsgegevens op straat

- **Voorbeeld:** Een museum organiseert een grote tentoonstelling en verzamelt persoonlijke gegevens van de bezoekers via een online ticketingsysteem. Zonder goede beveiliging is er een risico dat het systeem wordt het systeem gehackt, en kunnen namen, e-mails en betalingsgegevens op straat komen te liggen. Let op: indien dit gebeurt dan moet dat binnen 72 uur gemeld worden bij de Autoriteit Persoonsgegevens.

- **Impact:** Schade aan reputatie, verlies van bezoekersvertrouwen, en boetes onder de AVG.

2. Toegang tot digitale collecties verloren

- **Voorbeeld:** Een archief beheert zeldzame gedigitaliseerde kunstwerken. Een ransomware-aanval versleutelt alle bestanden, waardoor de organisatie geen toegang meer heeft tot deze digitale collecties.

- **Impact:** Permanente of tijdelijke verlies van waardevolle data, hoge kosten om toegang terug te krijgen, en mogelijk verlies van subsidie door nalatigheid.

3. Publieke onrust door sabotage van klimaatsystemen

- **Voorbeeld:** De klimaatbeheersing in een museum wordt digitaal aangestuurd. Een kwaadwillende partij krijgt toegang tot deze systemen en manipuleert de temperatuur en luchtvochtigheid, waardoor kunstwerken beschadigd raken.

- **Impact:** Onherstelbare schade aan erfgoed en reputatieschade richting sponsoren en partners.

4. Ticketsysteem plat door een DDoS-aanval

- **Voorbeeld:** Tijdens een groot evenement wordt het ticketsysteem van een theater getroffen door een Distributed Denial of Service (DDoS)-aanval. Bezoekers kunnen geen tickets kopen en toegang wordt chaotisch geregeld.

- **Impact:** Financieel verlies door gemiste ticketverkoop, frustratie bij bezoekers, en extra druk op het personeel.

5. Misbruik van inloggegevens door leveranciers

- **Voorbeeld:** Een externe leverancier die onderhoud uitvoert op een database heeft onvoldoende beveiliging op hun eigen netwerk. Cybercriminelen krijgen via deze zwakke schakel toegang tot het systeem van de culturele instelling.

- **Impact:** Blootstelling van gevoelige informatie en verstoring van bedrijfsprocessen.

6. Nepmailcampagne leidt tot phishing

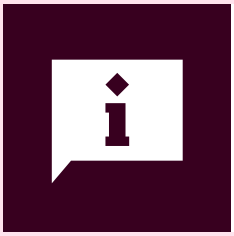
- **Voorbeeld:** Hackers versturen nep-e-mails uit naam van een bekende culturele instelling met een verzoek om donaties voor een “restauratieproject”. Bezoekers trappen erin en verliezen geld.

- **Impact:** Schade aan vertrouwen van het publiek en juridische complicaties.

7. Bedrijfsstilstand door verlies van sleuteltoegang

- **Voorbeeld:** De IT-afdeling verliest door een cyberincident toegang tot SaaS-oplossingen die gebruikt worden voor salarisadministratie en evenementplanning.

- **Impact:** Salarissen worden niet uitbetaald, geplande evenementen raken in de war, en het personeel ervaart onrust.



Op het moment dat je jouw kroonjuwelen goed in zicht hebt, is het mogelijk om te bepalen hoe je deze wil gaan beschermen én wat je daarvoor over hebt. Het stelt je bovendien in staat om keuzes te maken waardoor je meer in controle komt over jouw informatie en processen. Deze keuzes zijn gebaseerd op de mate waarin je als organisatie bereid bent risico’s te accepteren.

Stap 2

Wat is jouw risico acceptatie?

Zodra je jouw kroonjuwelen hebt geïdentificeerd, kun je gerichte maatregelen nemen om ze te beschermen. Hierdoor wordt informatiebeveiliging behapbaar en voorkom je onnodige risico's. Risico's zijn onvermijdelijk, maar niet alle risico's zijn gelijk. Als organisatie moet je bepalen welke risico's je bereid bent te accepteren en welke niet. Dit noemen we risicoacceptatie. Het gaat hierbij om het vinden van een balans tussen het nemen van maatregelen, de kosten ervan, en de impact die een risico kan hebben.

Bij het identificeren van risico's, stel je jezelf de volgende vragen:

- **Wat kan er misgaan?**
  Denk aan datalekken, verlies van digitale collecties, of uitval van systemen tijdens een evenement.

- **Hoe groot is de kans dat het gebeurt?**
  Phishing mails zijn bijvoorbeeld bij sommige musea aan de orde van de dag. Hoe groot is de kans dat dit een keer misgaat?

- **Hoe ernstig is de impact?**
  Een voorbeeld hierbij is het verlies van ticketgegevens. Het verlies kan financiële schade en reputatieschade veroorzaken, terwijl uitval van je digitale archief tot onherstelbare schade kan leiden.

Op basis van deze analyse bepaal je welke risico's je accepteert en welke je wilt beperken. Bijvoorbeeld:

- Voor kleinere risico's kies je ervoor om ze te **accepteren** en geen extra maatregelen te nemen.

- Grotere risico's kun je **verleggen** door verzekeringen af te sluiten of verantwoordelijkheid te delen met leveranciers via duidelijke afspraken en Service Level Agreements.

- Voor kritieke risico's, zoals het beschermen van persoonsgegevens of kunstwerken, neem je maatregelen om ze zoveel mogelijk te **vermijden** of te **beheersen**.

Bij risicoacceptatie is het belangrijk dat dit een bewuste keuze is, uiteindelijk gemaakt door de directie. Documenteer deze keuzes en zorg dat ze regelmatig worden geëvalueerd. Zo blijf je grip houden op wat écht belangrijk is voor jouw organisatie en voorkom je verrassingen.

Stap 3

Beheersmaatregelen implementeren

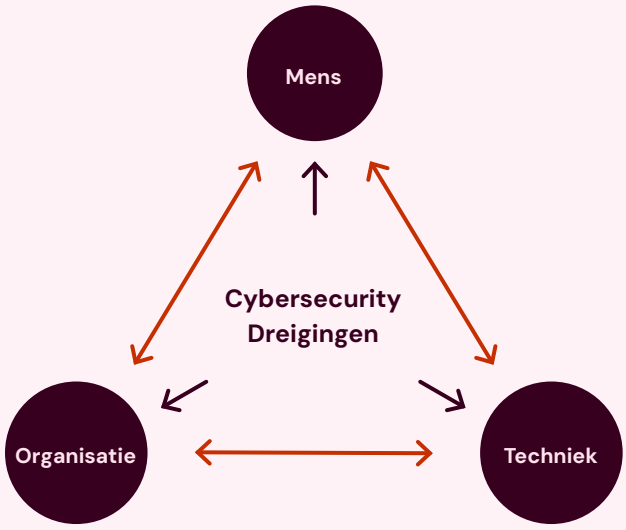
Wanneer je weet welke risico's je wilt beperken, is het tijd om beheersmaatregelen te implementeren. Dit betekent dat je gericht actie onderneemt om jouw kroonjuwelen te beschermen tegen bedreigingen en verstoringen. Denk hierbij aan de volgende onderwerpen:

- **Governance:** betreft procedures, en eigenaarschap. Wijs voor elk kritisch proces of systeem een interne eigenaar aan. Deze persoon is verantwoordelijk voor het beheer, hieronder valt ook contractmanagement met externe partijen, en de beveiliging ervan. Zonder eigenaarschap dreigen maatregelen verloren te gaan in de dagelijkse praktijk. Stel ten slotte procedures op om snel en adequaat te reageren als er iets misgaat. Denk aan duidelijke stappen voor het afhandelen van een cyberincident of datalek, inclusief escalatieprocedures en contactinformatie van betrokkenen. Maak het duidelijk wie medewerkers moeten bellen als apparaten niet meer werken, of als ze per ongeluk toch op een phising-mail gereageerd hebben.

- **Beleid:** Zorg er daarnaast voor dat dat er beleid is voor alle vormen van informatieopslag. Indien je software van een externe partij afneemt (Software as a Service, SaaS) dan stel je eisen aan leveranciers, zoals sterke beveiligingsprotocollen en een gedetailleerd Service Level Agreement (SLA). Op de website van Digital Trust Center staat een checklist voor het opstellen van een SLA. Voor papieren documenten geldt dat ze veilig opgeborgen worden en toegang beperkt is.

- **IT-security:** Neem technische maatregelen zoals netwerksegmentatie en sterke authenticatiemechanismen. Door gevoelige gegevens en systemen te isoleren van andere delen van je netwerk, beperk je de kans op een groot datalek.

- **Awareness:** de mens is de sterkste maar ook de zwakste schakel. Je kunt stap 1 en stap 2 wel op orde hebben maar als je niet met een doorlopend programma de awareness traint, toetst en monitort ben je alsnog heel kwetsbaar.



Het implementeren van zowel technische als organisatorische beheersmaatregelen vraagt om samenwerking tussen afdelingen. IT, functioneel beheer, en directie. Zij moeten gezamenlijk optrekken om maatregelen goed in te richten en regelmatig te evalueren. Zo zorg je ervoor dat jouw organisatie weerbaar is tegen de belangrijkste risico's.

Bron: Groeiboek cybersecurity (Groeiboek Cybersecurity tunnels - versie 2023 - COB)

Stap 4

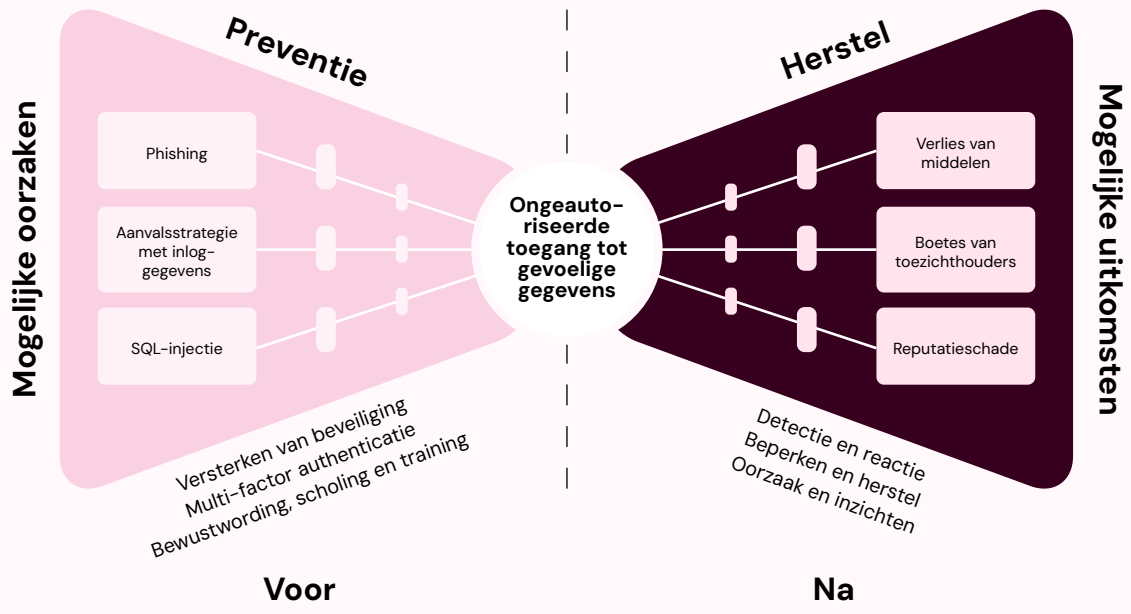
Monitoring, training en evaluatie

Het implementeren van beheersmaatregelen is een belangrijke stap, maar informatiebeveiliging stopt daar niet. Monitoring, training en evaluatie zijn cruciaal om ervoor te zorgen dat je beveiliging up-to-date blijft en je effectief blijft inspelen op nieuwe bedreigingen en ontwikkelingen.

Een goede aanpak voor monitoring en evaluatie omvat de volgende elementen:

- **Regelmatige procescontroles:** Controleer periodiek of processen nog voldoen aan de gestelde eisen en of beheersmaatregelen goed worden uitgevoerd. Dit voorkomt dat beveiliging verslapt of niet meer aansluit bij de praktijk.

- **Gebruik van visuele modellen:** Tools zoals het bow-tie model helpen om risico's inzichtelijk te maken (Je kunt een variant op onderstaande afbeelding gebruiken). Met dit model breng je zowel oorzaken van incidenten als de gevolgen in kaart, zodat je proactief kunt werken aan het verminderen van risico's.



Gebaseerd op het model: How to assess security risks using the bow tie method
(How to assess security risks using the bow tie method – Cyber Security Leadership)

- **Audits:** Indien je een bepaalde mate van volwassenheid bereikt hebt dan is het verstandig om je organisatie te onderwerpen aan verschillende vormen van toetsing, denk hierbij aan officiële audits, penetratietesten van je systemen en RED-teaming. RED-teaming zijn simulaties waarbij een 'aanvallend team' zwakke plekken opspoort in je systemen en processen. Audits doe je ten behoeve van jezelf om te kijken hoe cyber veilig je bent en deze verschillende vormen van toetsing geven waardevolle inzichten in kwetsbaarheden die anders onopgemerkt blijven.

Naast deze maatregelen is het essentieel om een cultuur van continue verbetering en veilige sfeer te omarmen. Je collega's moeten zich durven uit te spreken als zij per ongeluk op een link geklikt hebben want alleen dan kan een organisatie snel handelen en kun je de gevolgschade nog enigszins beperken.

Analyseer incidenten en verstoringen niet alleen om problemen op te lossen, maar ook om hiervan te leren en toekomstige incidenten te voorkomen. Dit proces, vaak aangeduid als probleemmanagement, helpt onderliggende oorzaken te identificeren en structurele oplossingen te implementeren.

Door monitoring en evaluatie goed in te bedden in je organisatie, creëer je een dynamisch en toekomstbestendig beveiligingsbeleid. Zo blijf je voorbereid op nieuwe risico's en bescherm je jouw kroonjuwelen optimaal.

Meer weten over Cyberveiligheid?

Check de site van DEN, het kennisinstituut voor digitale transformatie in de culturele sector. Op de site vind je bijvoorbeeld de **Cyberveilig check**, een online tool om na te gaan hoe cyberveilig jouw organisatie is.

Het stappenplan Cyberveiligheid in culturele organisaties gaat in op belangrijkste punten. Het is niet compleet en uitputtend. Kijk voor meer informatie over cyberveiligheid in de culturele sector op **www.den.nl**.