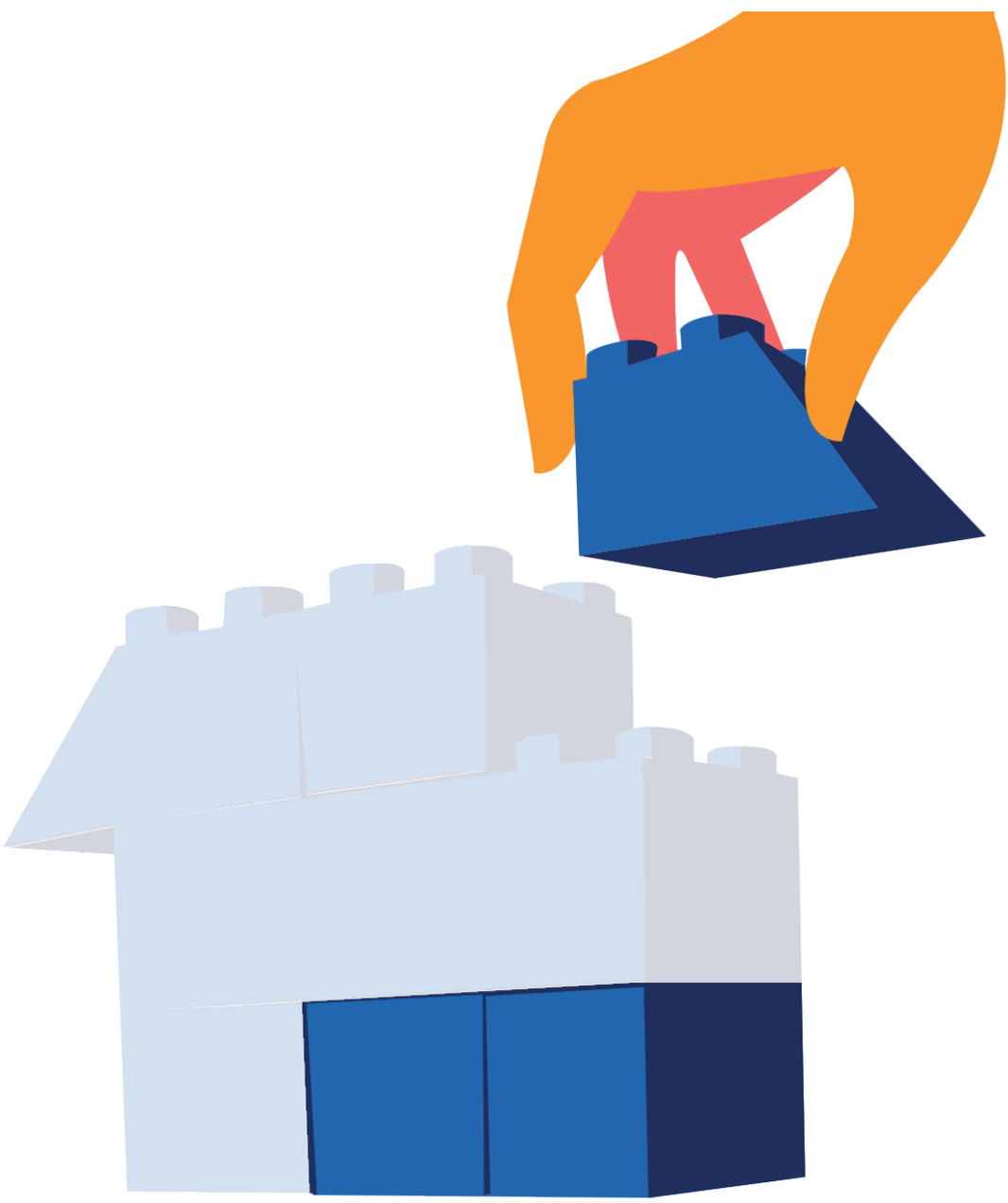
Audittrail
information security | privacy | quality | grc

BIC Building Blocks Implementeren & Bijsturen



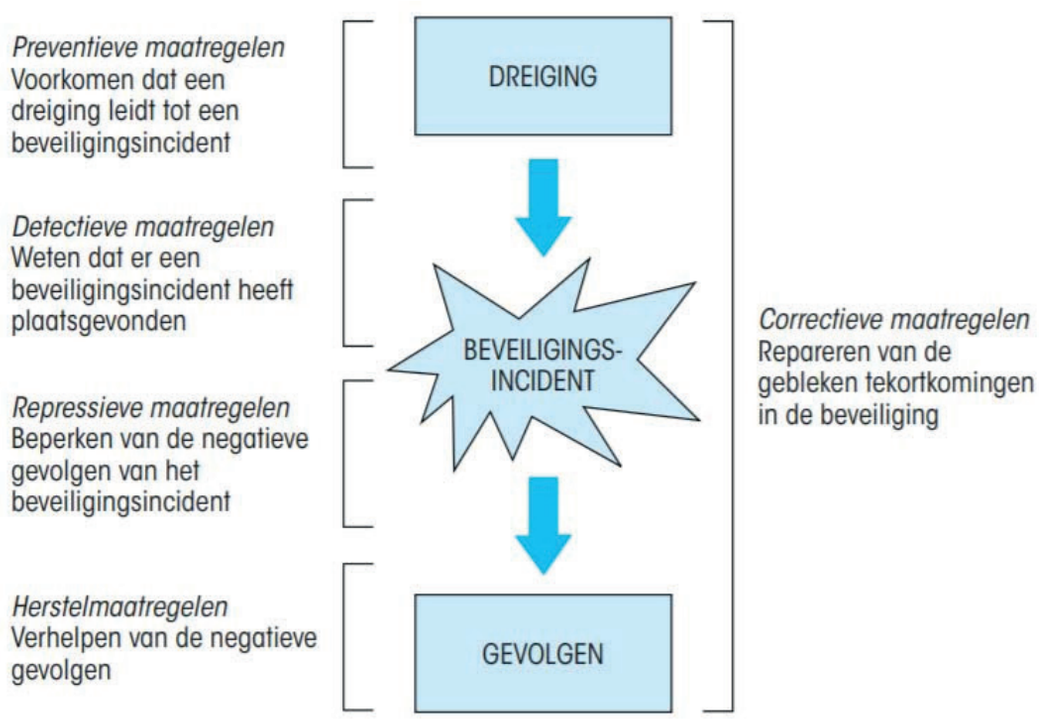
IMPLEMENTEREN EN BIJSTUREN

Nu de scope helder is, verantwoordelijkheden zijn belegd en zowel informatie als risico's zijn geïnventariseerd is het tijd om maatregelen te implementeren binnen de organisatie. Hoe komt u nu tot een set maatregelen die de risico's van uw corporatie mitigeert en wanneer spreekt men daadwerkelijk van een 'passende beveiliging'? In dit whitepaper onderzoeken we het implementeren van informatiebeveiligingsmaatregelen en het bijsturen ervan.

SOORTEN MAATREGELEN

Informatiebeveiliging wordt ingericht aan de hand van een normenkader dat een breed scala aan maatregelen aanbiedt. Anders dan bij een wetgeving is een organisatie vrij om deze maatregelen zelf op waarde te schatten en om een eigen set maatregelen te implementeren die past bij de organisatie en de informatie die zij heeft. Het volgen van een normenkader als de BIC – dat een basis biedt voor informatiebeveiliging - volgt een 'pas toe of leg uit' principe. Wat wil zeggen dat je als organisatie zelf kiest of je maatregelen wel of niet implementeert. Maar, wanneer je iets niet doet je wel beargumenteerd waarom niet. Dit kan bijvoorbeeld zijn omdat er al voldoende aanvullende maatregelen zijn ingericht of omdat de maatregel niet bijdraagt aan het mitigeren van de risico's op de risicokaart van de organisatie.

De BIC kent een groot aantal aan maatregelen, die kunnen worden onderverdeeld in onderstaande soorten.



MAATREGELEN DIE EEN PASSEND BEVEILIGINGSNIVEAU GARANDEREN

ESSENTIËLE MAATREGELEN

NEN geeft een mooie checklist als het gaat om het implementeren van de belangrijkste essentiële maatregelen binnen een organisatie. Met deze twaalf domeinen voor maatregelen bent u al een eind op weg met informatiebeveiliging binnen de organisatie!

1. STEL INFORMATIEBEVEILIGINGSBELEID OP

Goed dat NEN hiermee begint! Zonder beleid, geen structuur. Het opstellen van beleid hebben we met de BIC al behandeld in het eerste hoofdstuk: Beleid en strategie. Een eerste horde is dus al genomen.

2. STEL VAST WIE WAARVOOR VERANTWOORDELIJK IS

Ook de verantwoordelijken zijn reeds vastgesteld en zijn misschien al bijeen gebracht in een regiegroep.

3. ZORG VOOR BEWUSTWORDING, OPLEIDING EN TRAINING

Het informeren en opleiding van medewerkers is een belangrijke stap in informatieveilig werken. Natuurlijk is een deel af te dwingen met techniek en het op passende wijze faciliteren van de medewerkers, maar informatiebeveiliging is toch echt grotendeels mensenwerk. Zorgen voor bewustwording gaat niet alleen over een enkele campagne of actie, maar zal een programma vereisen: bewust-worden en bewust-zijn vereist constante aandacht.

4. NEEM MAATREGELEN TEGEN KWAADAARDIGE PROGRAMMATUUR

Als alle medewerkers op de hoogte zijn van beleid en hoe informatieveilig te werken, dan is ook van belang dat derden met kwade bedoelingen niet alsnog in bezit komen van gegevens. De meeste dreigingen van derden komen van internet en vallen daarmee onder cyber bedreigingen. Denk hierbij aan malware in de vorm van ransomware, virussen, maar ook (spear) phishing valt hieronder. Dit bedreigt niet alleen de pc of laptop, houdt ook rekening met mobiele telefoons en tablets. Zorg dat goede anti-virussoftware is geïnstalleerd en houdt updates nauwkeurig bij (regelmatig komen updates beschikbaar juist omdat er een lek in de beveiliging is aangetroffen!).

5. SLUIT OVEREENKOMSTEN VOOR GEGEVENSUITWISSELING

Denk hierbij niet alleen aan verwerkersovereenkomsten in het kader van privacy, ook andere typen informatie zijn de moeite waard om goede afspraken over te maken. Denk hierbij ook aan leveranciers van SAAS/cloud applicaties en infrastructuur. Maak heldere afspraken met leveranciers waar verantwoordelijkheden met betrekking tot informatiebeveiliging liggen en wat je verwacht van de andere partij op het gebied van beschikbaarheid, vertrouwelijkheid en integriteit van de informatie die zij voor uw corporatie verwerken of bewerken. De eisen die u stelt aan leveranciers kunnen per partij verschillen, afhankelijk van de classificatie van de gegevens en de risicokaart van uw organisatie. Leg afspraken duidelijk vast in verwerkersovereenkomsten, SLA's of DAPs. Monitor de uitvoering van de afspraken en evalueer periodiek om bij te kunnen stellen.

6. BEVEILIG DE TOEGANG TOT SYSTEMEN

In theorie is digitale informatie benaderbaar op elk moment, vanaf elke locatie en voor iedereen. De vraag is eerder: is dit ook wenselijk? Toegang tot informatie is afhankelijk van de classificatie van deze informatie: wie mag erbij (en wie dus niet)? Is een enkele inlog voldoende, of is een extra authenticatie vereist? En mag iedereen de informatie vanaf elke locatie benaderen, of zijn sommige typen informatie bijvoorbeeld alleen toegankelijk vanuit kantoor? Naast het autoriseren van de juiste personen voor toegang tot de juiste informatie is het ook van belang medewerkers duidelijk te maken dat ze hun identificatie en authenticatiemiddelen niet overdragen aan anderen.

Audittrail
information security | privacy | quality | grc

ESSENTIËLE MAATREGELEN - VERVOLG

7. ONTWIKKEL EN IMPLEMENTEER CONTINUÏTEITSBEHEER

Continuïteitsbeheer is een van de belangrijkste componenten van informatiebeveiliging: zorgdragen dat de informatievoorziening zonder onderbreking doorloopt. Om deze continuïteit te waarborgen kunnen veel verschillende maatregelen worden genomen. Denk hierbij aan back-ups en eventueel dubbele uitvoering (redundatie) van omgeving, noodstroomvoorzieningen, uitwijkmogelijkheden etc. Zorg dat er een continuïteitsplan ligt die rekening houdt met de risicokaart van de organisatie en dat dit periodiek wordt getest. Als het beheer van de IT organisatie is uitbesteed aan een derde partij, neem dan ook het continuïteitsbeheer mee in de afspraken met de leverancier.

8. HOUD REKENING MET INTELLECTUEEL EIGENDOM

Houd licenties bij en zorg dat er geen illegale software in omloop komt. Het gebruik van illegale software heeft twee nadelen. Ten eerste is de herkomst veelal schimmig, waardoor eenvoudig kwaadaardige programmatuur kan binnensluipen. Ten tweede kunnen rechthebbenden bij vermoeden van inbreuk op intellectuele rechten, onmiddellijke inbeslagname vorderen van de apparatuur waarop de software zich bevindt. Verder spelen andere risico's mee, zoals strafrechtelijke vervolging en reputatieschade.

9. BEVEILIG BEDRIJFSDOCUMENTEN

Belangrijke bedrijfsdocumenten moeten worden beveiligd tegen verlies, vernietiging en vervalsing. Elektronisch opgeslagen gegevens moeten 'digitaal duurzaam' zijn, eventuele encryptiesleutels moeten ook worden bewaard en gegevens moeten kunnen worden opgevraagd en overgedragen.

10. BESCHERM PERSOONSGEGEVENS

In het algemeen volgt de plicht tot bescherming van persoonsgegevens uit artikel 32 van de AVG. Hierin wordt gesproken over een passende beveiliging van deze gegevens. Wat dit precies betekent voor de beveiliging, is afhankelijk van het type persoonsgegevens. Algemene gegevens, bijvoorbeeld afkomstig van visitekaartjes, zullen een andere classificatie krijgen dan gegevens over huurschulden of overlast. Houdt met deze classificatie ook rekening bij het stellen van eisen aan Verwerkers.

11. LEEF BEVEILIGINGSBELEID NA

Het klinkt logisch. Naleving is echter alleen te toetsen door middel van controles. Hoe u deze controles inricht is afhankelijk van de organisatie en verantwoordelijkheden. Misschien worden bij u intern controles uitgevoerd door een interne auditafdeling, de controlafdeling, of is het de informatiebeveiliger zelf die controles uitzet binnen de organisatie. Naast interne controles is het ook aan te bevelen om periodiek een derde partij een objectieve en onpartijdige controle te laten uitvoeren.

12. RAPPORTEER BEVEILIGINGSINCIDENTEN

Incidenten maken de organisatie beter – mits ze worden gemeld en verbetermaatregelen worden opgevolgd! Een beveiligingsincident heeft te maken met het niet volledig of niet juist werken van een geïmplementeerde maatregel. Daarom is het belangrijk deze incidenten altijd te onderzoeken en de maatregel waar ze betrekking op hebben aan te passen door middel van verbetermaatregelen.

Contactgegevens
Audittrail
Sisalbaan 5a
2352 AE Leiderdorp

KantNoord
Winschoterdiep 50
9723 AB Groningen

071 - 747 71 71
BBB@audittrail.nl

Audittrail
information security | privacy | quality | grc