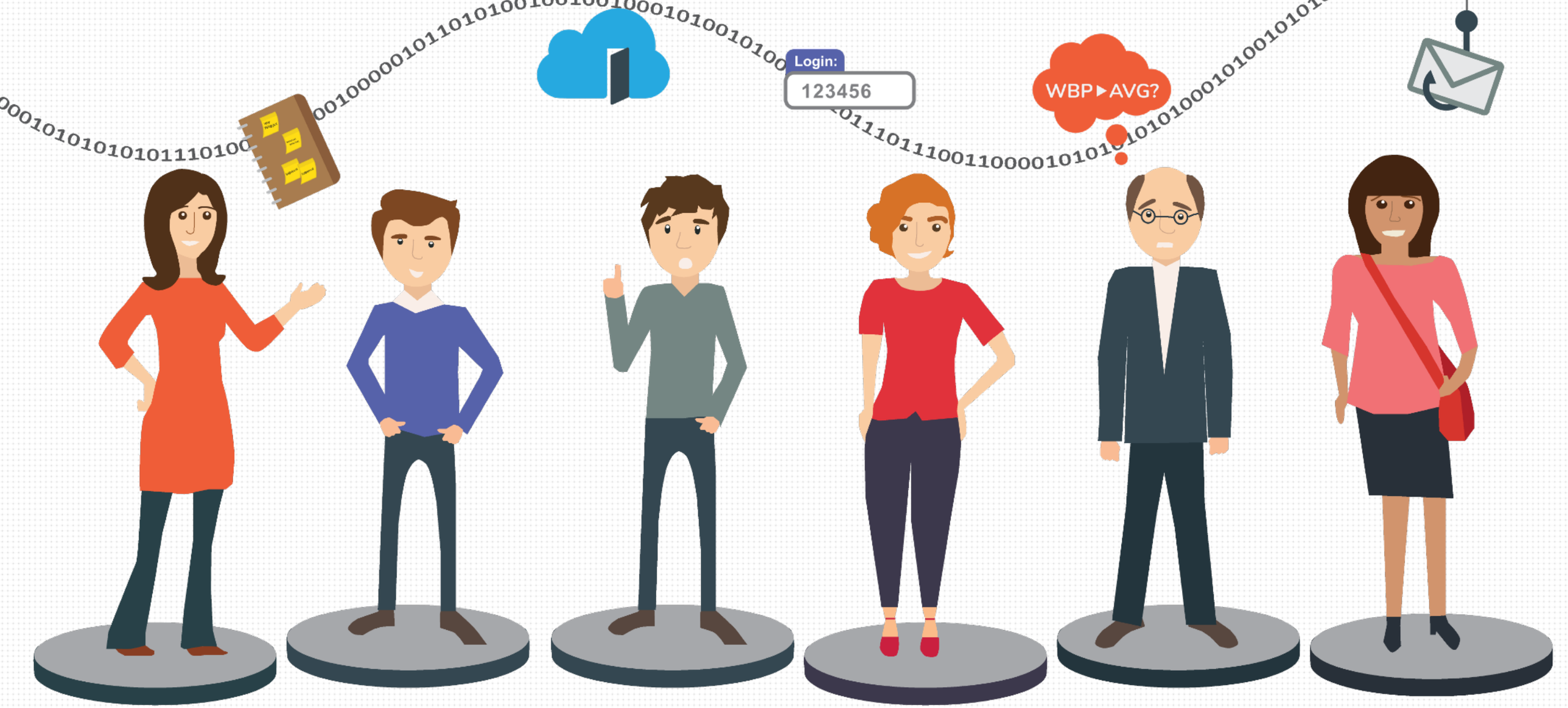
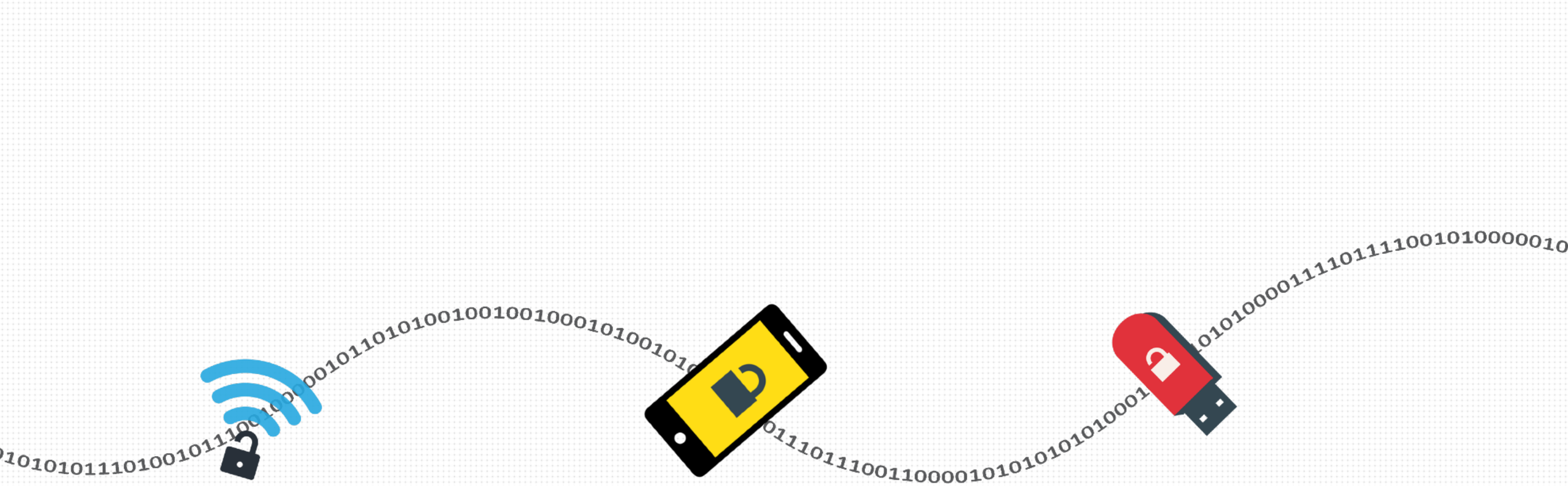
hutspot

LBVD

Hutspot & LBVD aanpak voor IBP

Hoe veilig is jouw informatie?





hutspot

LBVD

IBP in het onderwijs

Scholen houden steeds meer (persoons)gegevens bij over studenten en medewerkers. Ook wordt in de samenwerking met externe partijen steeds vaker (persoons)gegevens uitgewisseld. Als school heb je de verantwoordelijkheid om zorgvuldig met die gegevens om te gaan. Dat vraagt om aandacht voor Informatiebeveiliging en Privacy (IBP). Hutspot en LBVD bieden scholen een passende aanpak om daar grip op te krijgen!

IBP is een onderwerp dat, mede onder invloed van veranderende Europese wetgeving met financiële sancties, in korte tijd hoog op de agenda van mbo-scholen is komen te staan. Studenten en medewerkers mogen ervan uitgaan dat de school hun gegevens goed en vertrouwelijk behandelt. Daarnaast is het van groot belang dat de kerntaak van het mbo-onderwijs, het geven van goed onderwijs en het diplomeren van studenten, op een betrouwbare en correcte wijze wordt uitgevoerd. Diploma's zijn maatschappelijk van grote waarde en mogen niet ter discussie komen te staan.

Mens, organisatie en techniek in balans

Wij geloven dat je met IBP zorgt voor een veilige en leefbare werk- en leeromgeving waarbinnen de kerntaak van het onderwijs zorgvuldig kan worden uitgevoerd. En dat je daar komt door aan de slag te gaan met de mensen in de organisatie, de organisatie zelf én de techniek. Het gaat om bewustwording, gedrag en cultuur (mens), beleid, kaders en duidelijke procedures (organisatie) én passende ICT maatregelen (techniek).

Inzetten van kennis en ervaring

Hutspot en LBVD zijn de partij die hierbij kunnen helpen. Hutspot helpt met organisatievraagstukken in het onderwijs, is goed in het combineren van inhoud en proces en het realiseren van verandering. LBVD is een expert op het gebied van informatiebeveiliging en heeft een aantal effectieve tools ontwikkeld om hiermee aan de slag te gaan.

Samen helpen wij scholen met een pragmatische aanpak om grip te krijgen en de eerste stappen te zetten op het vlak van IBP. Zijn er al stappen gezet en/of wil je graag op een specifiek onderdeel de diepte in? Ook daar hebben wij een antwoord op. Onze aanpak wordt in dit boekje uitgebreid toegelicht.

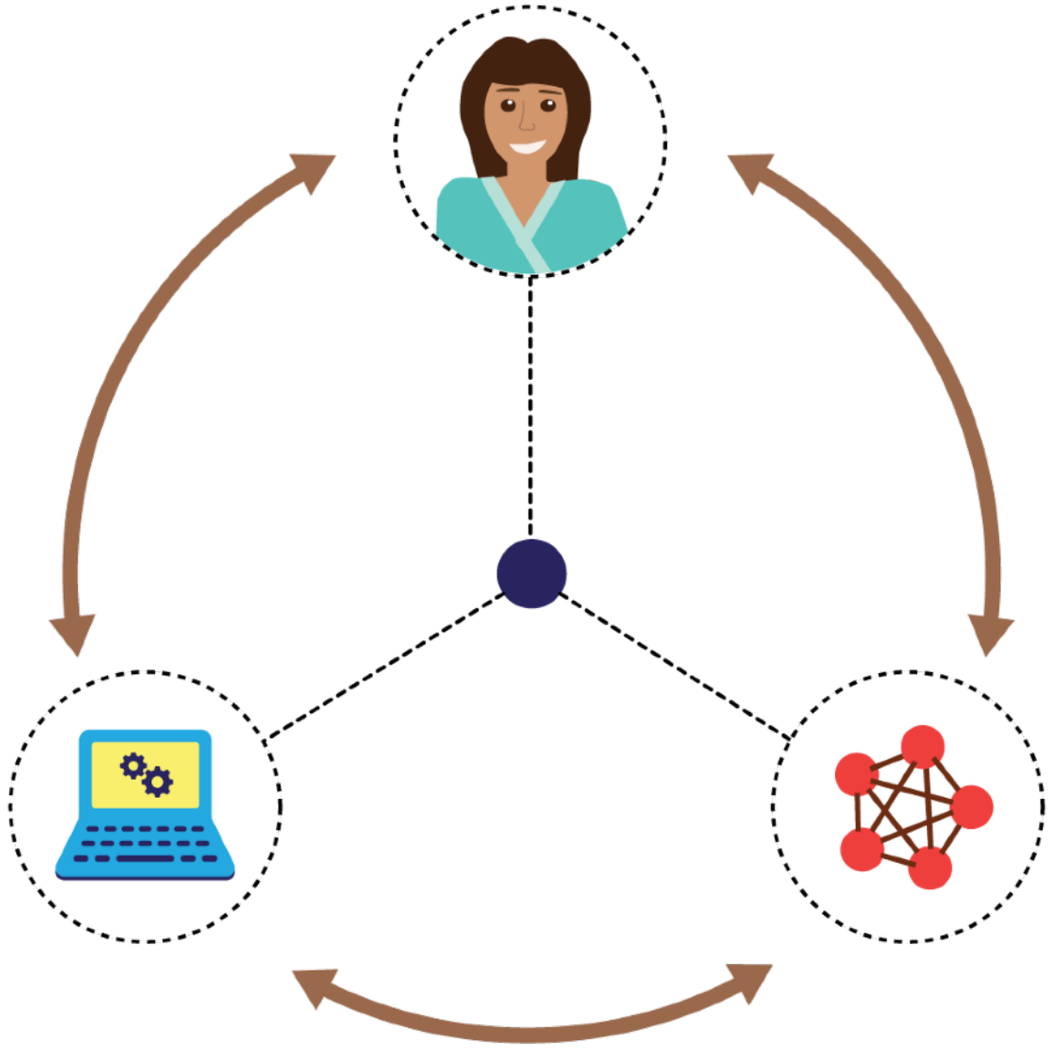
IBP krijgt veel aandacht in de sector. Hierdoor hoeven we niet het wiel opnieuw uit te vinden, maar kunnen we gebruik maken van wat er al is. Zo is er een Framework IBP opgezet, dat gevuld is met allerlei materiaal op het gebied van IBP, zoals het speciaal voor het mbo ontwikkelde IBP Normen- en Toetsingskader. Het materiaal uit het Framework passen wij op diverse manieren toe.

hutspot

LBVD

Mens

bewustwording, gedrag,
eigen verantwoordelijkheid



Techniek

ICT maatregelen, veilige en beschikbare systemen

Organisatie

kaders, beleid en heldere procedures

hutspot
LBVD

Aanpak

Alle mbo-scholen moeten de komende tijd aan de slag met IBP om in mei 2018 te kunnen voldoen aan nieuwe wet- en regelgeving. Met een goede aanpak voor IBP kun je zorgen voor een veilige werk- en leeromgeving. Je komt daar, door aan de slag te gaan met de mensen, de organisatie én de techniek. Hoe ver een organisatie met IBP is en waar de aandachtspunten liggen, verschilt per school.

Afhankelijk van waar de organisatie staat en wat de behoefte is, kunnen Hutspot en LBVD op verschillende manieren helpen.

Bijvoorbeeld:

- **Door een fundament neer te leggen**: in de breedte de eerste stappen zetten met IBP, met aandacht voor mens, organisatie en techniek.
- **Door het uitbouwen van de basis**: stevig aan de slag op specifieke onderdelen zoals bewustwording, in kaart brengen van risico's of een systeemtest. We kunnen de diepte in op onderdelen die bij het neerleggen van een fundament juist op hoofdlijnen aan de orde komen.
- **Door IBP in te bedden in de organisatie**: het maken van een plan voor de realisatie van lange termijn maatregelen en/of het structureel borgen van het IBP-proces in de organisatie.

In dit boekje lichten we toe hoe we met een aanpak op hoofdlijnen een fundament neerleggen, wat we bedoelen met het uitbouwen van specifieke onderdelen en hoe IBP een vaste plek in de organisatie kan krijgen. Natuurlijk is er bij de uitwerking ruimte voor een schooleigen invulling. Samen kijken we naar wat het beste past bij de vraag en de organisatie.

Resultaten die geboekt worden:

- mensen zijn zich **bewust** van het belang en de risico's, begrijpen en nemen hun eigen verantwoordelijkheid daarin en gaan zich daar uiteindelijk naar gedragen.
- door de organisatie vastgestelde kaders zijn doorvertaald naar **beleid** en **procedures**.
- passende technische maatregelen borgen dat belangrijke systemen voldoende **beveiligd** en **beschikbaar** zijn.

hutspot

LBVD

hutspot

LBVD

Fundament neerleggen

Stap 1 Informatiecampagne voor bewustwording

Met een informatiecampagne maken we medewerkers bewust van de relevantie van IBP, de risico's en de manier waarop zij zelf een bijdrage kunnen leveren aan een veilige werk- en leeromgeving. We zetten een aantal gerichte communicatiemiddelen in met als doel om zoveel mogelijk medewerkers te bereiken en te zorgen dat ze in de hoofdlijn weten waar IBP over gaat en waarom het relevant is voor de school. We communiceren met impact en besteden daarom aandacht aan de uitstraling en vormgeving van de boodschap.

Stap 2 Risico's IBP in beeld

We organiseren twee workshops waarin we een risicoanalyse op hoofdlijnen uitvoeren. Het doel is om een eerste inzicht te krijgen in de risico's en de prioriteiten. Met een representatieve groep medewerkers inventariseren en prioriteren we op basis van het 'Framework' en 'IBP Normenkader mbo' de risico's voor de eigen organisatie. Het resultaat is een prioritering van risico's die voor de school om maatregelen vragen. Tijdens een brainstorm inventariseren we vervolgens mogelijke maatregelen. Met deze aanpak werken we tegelijkertijd aan draagvlak voor het onderwerp en aan mogelijke oplossingen op de korte en lange termijn.

Stap 3 Direct aan de slag met reductie van risico's

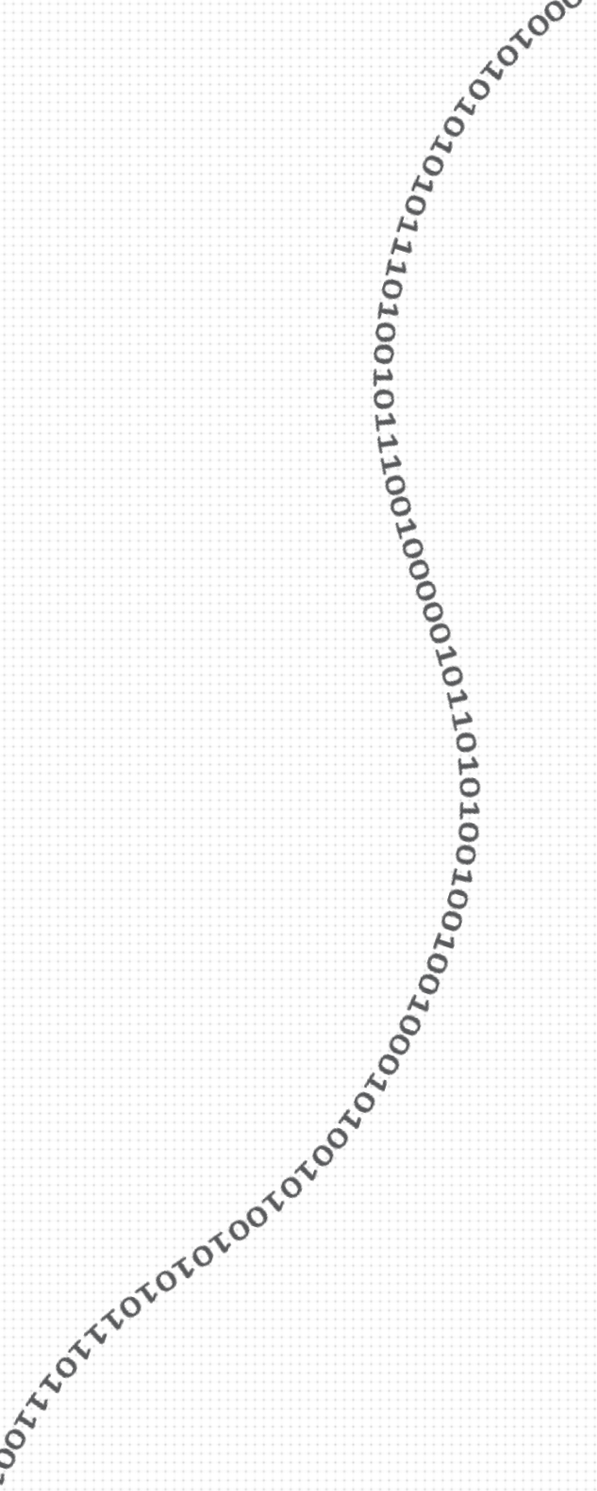
De brainstorm over maatregelen geeft inzicht in snel te realiseren maatregelen die met beperkte inzet van tijd en geld de risico's verminderen of wegnemen. Wij helpen scholen bij het realiseren van deze quick-wins. Door de opdracht voor het realiseren van de maatregel, met scherpe opdrachtomschrijving, mee te geven aan de juiste persoon in de organisatie en hulp te bieden bij de realisatie. Óf door de realisatie desgewenst zelf op te pakken.

Stap 4 Vervolgstap aanpak (midden)lange termijn

De risicoanalyse geeft handvatten voor het uitwerken van de gewenste situatie op de (midden)lange termijn. Het doel is om de hoogst geprioriteerde risico's terug te brengen naar een gewenst niveau. De risico's, prioriteiten en maatregelen zetten we af tegen de middelen die de school beschikbaar wil en kan stellen. Wij helpen bij het bepalen van het startpunt, de stip op de horizon en het bijbehorende tijdpad. Het plan van aanpak dat daaruit volgt, geeft inzicht in welke maatregelen worden gerealiseerd, voor welke risico's, met welke middelen, in welk tijdpad en wie de verantwoordelijk draagt.

Met stap één tot en met vier wordt in +/- 6 maanden tijd een fundament neergelegd voor IBP binnen de school.

hutspot
LBVD


hutspot
LBVD

Uitbouwen: risicoanalyse

Uitbouwen met een verdiepende risicoanalyse

Het samen met collega's inventariseren van potentiële risico's op het gebied van IBP is een goede manier om inzicht te krijgen in de huidige stand van zaken en prioriteiten. Een risicoanalyse kunnen we beknopt uitvoeren (als onderdeel van het "fundament neerleggen") en we kunnen de diepte in. Met een uitgebreidere aanpak van de risicoanalyse worden risico's breder in de organisatie in kaart gebracht en kunnen we meer medewerkers betrekken.

Het wiel hoeft niet opnieuw te worden uitgevonden. Hutspot en LBVD combineren de beproefde RISMAN-methode voor risicoanalyses met reeds door saMBO-ICT geïnventariseerde risico's en het IBP Normenkader mbo. Zo kunnen we vlot met groepen medewerkers de risico's voor de school verkennen en maatregelen benoemen. Dat doen we in een aantal workshops met 10-15 deelnemers die een doorsnede zijn van medewerkers uit de organisatie.

Samen bepalen we de scope: is er behoefte om een specifiek onderdeel in kaart te brengen? Of juist om breed de risico's in beeld te brengen? De risicoanalyse start met het vaststellen van de ongewenste topgebeurtenis: hetgeen je wilt voorkomen! Bijvoorbeeld dat onbevoegden privacygevoelige informatie kunnen inzien en bewerken. De ongewenste topgebeurtenis is het vertrekpunt van de risicoanalyse. Aan deelnemers wordt gevraagd om vanuit verschillende invalshoeken (zoals organisatorisch, bestuurlijk, financieel en technisch) risico's te benoemen en/of voorgesorteerde risico's aan te vullen. De risico's worden geprioriteerd en er worden maatregelen geformuleerd waarmee de risico's teruggebracht kunnen worden naar een acceptabel niveau.

De uitkomst uit de risicoanalyse vatten we samen in een presentatie. De uitkomst geeft inzicht in risico's, maatregelen en prioriteiten. Tegelijkertijd wordt er gewerkt aan bewustwording van medewerkers. Zij beseffen welke risico's er spelen, waardoor draagvlak toeneemt voor de te nemen maatregelen en de prioriteiten.

De aanpak voor de risicoanalyse ziet er als volgt uit:

Stap 1: voorbereiding

- de ongewenste topgebeurtenis vaststellen;
- bepalen met wie de risicoanalyse wordt uitgevoerd;
- vaststellen programma, o.b.v. kennisniveau deelnemers;
- inrichten tools voor online ondersteuning bij het inventariseren en prioriteren van risico's en maatregelen.

Stap 2: uitvoeren workshops

- in verschillende workshops risico's aanvullen/ benoemen vanuit verschillende invalshoeken;
- risico's prioriteren per invalshoek of over invalshoeken heen;
- brainstormen over maatregelen.

Stap 3: verwerken resultaten

- rapportage van de resultaten;
- presentatie van de resultaten.

hutspot
LBVD

Uitbouwen: bewustwording

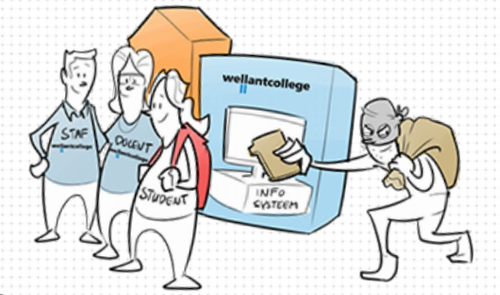
Uitbouwen met extra aandacht voor bewustwording

Werken aan bewustwording heeft als doel om het gedrag van medewerkers te beïnvloeden. Dat zorgt uiteindelijk voor een kleinere kans op incidenten. Denk aan zorgvuldige omgang met wachtwoorden, bewuste afwegingen voor het delen van informatie en betere beveiliging van bijv. USB-sticks en mobiele telefoons.

Gedragsveranderingen in organisaties vergen tijd en inspanning. Daarom stellen wij, bij het uitbouwen van bewustwording, een doelgroepgerichte benadering voor in 3 stappen. In stap 1 zorgen we voor een gedeeld kennisniveau over IBP bij alle medewerkers. Vervolgens gaan we in stap 2 en 3 verder met specifieke doelgroepen in de organisatie voor wie IBP een extra belangrijk aandachtsgebied is. Gezien hun rol en de informatie waarmee zij werken. Denk aan het management, de afdeling administratie, (een selectie van) ICT, docenten en aan zorgcoördinatoren.

Stap 1: Informatiecampagne voor gedeeld kennisniveau IBP

De informatiecampagne wordt breed in de organisatie uitgezet om zoveel mogelijk medewerkers te bereiken. Het doel is om mensen bewust(er) te maken van de relevantie van IBP voor de organisatie, de specifieke risico's, oplossingen voor de school en de eigen rol en verantwoordelijkheid daarin. We gaan in op persoons- en gevoelige gegevens, beleidskaders en regels en gebruik van ICT systemen. Tegelijkertijd wordt gewerkt aan draagvlak voor de maatregelen die mogelijk in een latere fase genomen moeten worden. De campagne wordt gevoed door onderwerpen die in het IBP Normenkader mbo als relevant zijn benoemd ten aanzien van bewustwording.



Informatiebeveiliging & Privacy

TIP:

WACHTWOORDEN ZIJN ALS ONDERGOED!

1. je laat ze niet slingeren
2. je wisselt ze regelmatig
3. je leent ze niet uit aan vreemden

hutspot

LBVD

Bij het ontwerpen van de informatiecampagne bepalen we samen wat de juiste boodschap is en welke middelen zorgen voor de gewenste impact. De boodschap en de middelen worden toegespitst op de verschillende belevingswerelden van de medewerkers. We besteden aandacht aan de uitstraling en vormgeving van de boodschap. Nooit als doel op zich, maar om de boodschap over te dragen. Daarbij maken we de afweging of we werken met bestaande middelen (intranet, nieuwsbrief, etc), juist nieuwe (animatie, infographic, tekeningen, etc) of met een combinatie.

Als alle medewerkers minimaal twee keer in aanraking zijn gekomen met IBP in de campagne gaan we door met interventies en workshops. Daarbij gaan we aan de slag met de groep medewerkers voor wie IBP een belangrijk aandachtsgebied is. Zij hebben door de campagne kennis genomen van het materiaal. Dit is een eerste voorbereiding op de interventies en workshops.

Stap 2: Interventies voor het ervaren van de noodzaak van IBP

Om gedragsverandering in gang te zetten is het nodig dat medewerkers het belang van IBP persoonlijk beleven. Dat zorgt er voor dat hun houding ten aanzien van het onderwerp verandert. Geen “ver van m’n bed show”, maar het komt dichtbij en het heft het gevoel van onschendbaarheid (het gaat niet over mij, dat overkomt mij niet) op. Een effectieve manier om dat te doen is om mensen gecontroleerd te confronteren met de noodzaak van IBP.

Er is een aantal manieren om dat te bereiken, bijvoorbeeld:

- **kennistoets** voor inzicht in het kennisniveau over IBP onder medewerkers;
- simuleren van een aanval met een **phishing e-mail** om te achterhalen hoe medewerkers daarmee omgaan;
- een **hack-demonstratie** om te laten zien hoe (eenvoudig) dit in zijn werk gaat;
- in een **risicoanalyse** samen grip krijgen op de IBP risico’s;
- met een **mystery guest** onderzoeken in hoeverre een onbevoegde toegang kan krijgen tot gevoelige informatie;
- begeleid spelen van de **game 'MBO Alert!** Privacy in de praktijk’.

Samen bedenken we welke interventies het meest passend zijn binnen de organisatie, de bestuurlijke kaders en hetgeen je als school wilt bereiken. De interventies zijn gericht op de doelgroepen waarmee we vervolgens ook de workshops in gaan. Zo krijgen de belevenissen uit de interventies betekenis.

hutspot
LBVD

Stap 3: Workshops voor doorvertaling van IBP naar de dagelijkse praktijk

Bij het in gang zetten van een gedragsverandering denken wij dat het noodzakelijk is om de doorvertaling te maken naar het dagelijkse werk van medewerkers. Daarbij spelen vragen zoals: wat zijn de belangrijkste IBP-aandachtspunten in mijn werk of in het werk van mijn afdeling? Hoe kan ik zelf risico's voorkomen? Welke afspraken maken we daar onderling over?

De workshops kunnen we starten met een groep leidinggevenden. Met de leidinggevenden worden, op basis van het huidige en/of in ontwikkeling zijnde beleid, kaders en uitgangspunten over IBP opgesteld. Waar beleid nog slechts papier is, worden in deze stap de belangrijke onderwerpen eruit gelicht. Deze uitspraken worden meegegeven in de verdiepende workshops voor specifieke doelgroepen medewerkers.

In de verdiepende workshops gaan we aan de slag op basis van het gedeelde kennisniveau en bespreken we de belevenissen uit de interventies. Gezamenlijk maakt de groep deelnemers een inventarisatie van waar IBP in hun werk over gaat. Daaruit komt naar voren welke zaken er spelen.

Bijvoorbeeld:

- met welke gevoelige (persoons)gegevens er gewerkt wordt;
- wie daarmee in aanraking komen;
- in welke vorm (fysiek of digitaal);
- via welke informatiesystemen;
- hoe toegangsbeveiliging en zaken als clean desk en clear screen georganiseerd zijn.

Vervolgens bepalen we samen met de medewerkers op welke manier hiermee omgegaan kan worden. Wat vraagt dat van het gedrag? Waar moet men op letten in het dagelijks werk? Dit leidt tot (werk)afspraken over gedrag en een eerste lijst met maatregelen om de IBP te verbeteren. De medewerkers kunnen hier binnen hun team direct mee aan de slag. Desgewenst vertalen we de resultaten naar overdraagbaar materiaal zoals een praatplaat of tekening.

	Stap 1	Stap 2	Stap 3
Aanpak	Informatie campagne	Interventies	Workshops
Doel	Weten	Beleven	Toepassen
Doelgroep	Alle medewerkers	Leidinggevenden Specifieke doelgroepen	Leidinggevenden Specifieke doelgroepen

Mate van bewustwording

hutspot
LBVD

hutspot

LBVD

Uitbouwen: ICT-systemen

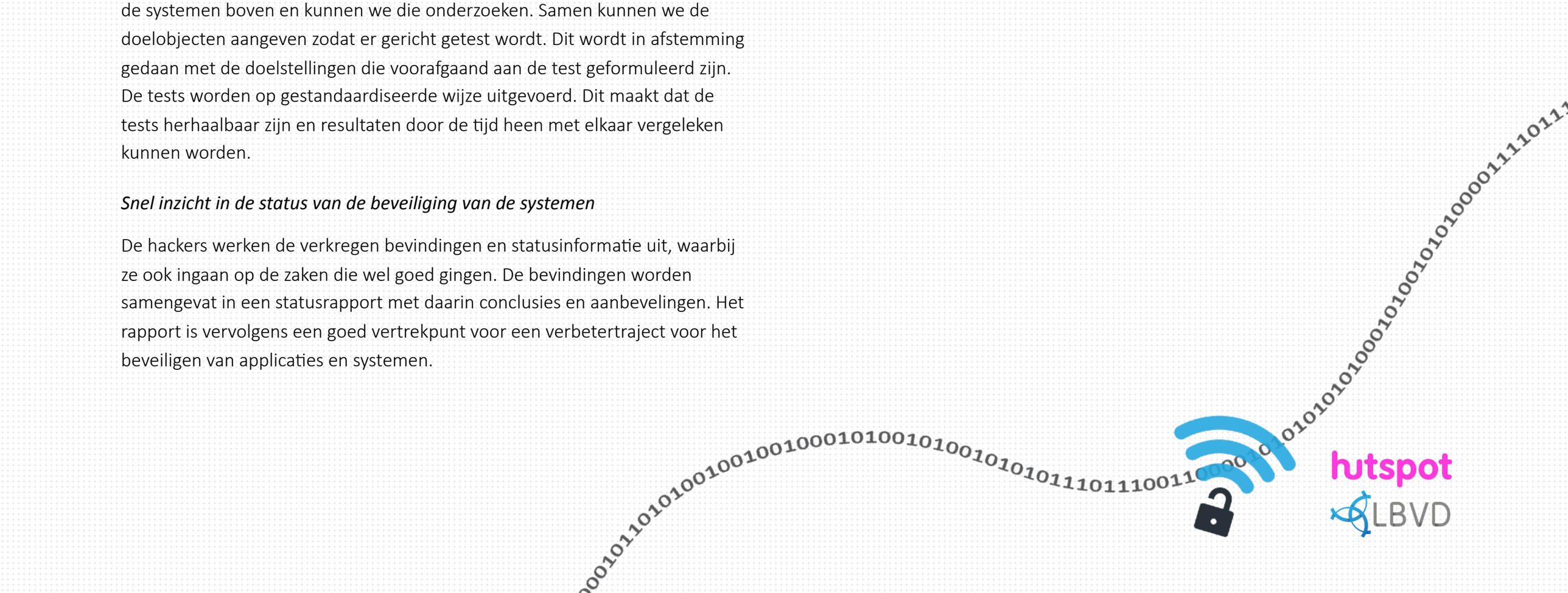
Uitbouwen met het op de proef stellen van eigen ICT-systemen

Als school wil je de informatievoorziening goed op orde hebben. Helaas komen cyberaanvallen veel voor. Als systemen niet goed genoeg zijn beveiligd kunnen kwaadwillenden gevoelige informatie bemachtigen. Om erachter te komen hoe veilig de schoolsystemen zijn, kunnen we die eens goed op de proef stellen.

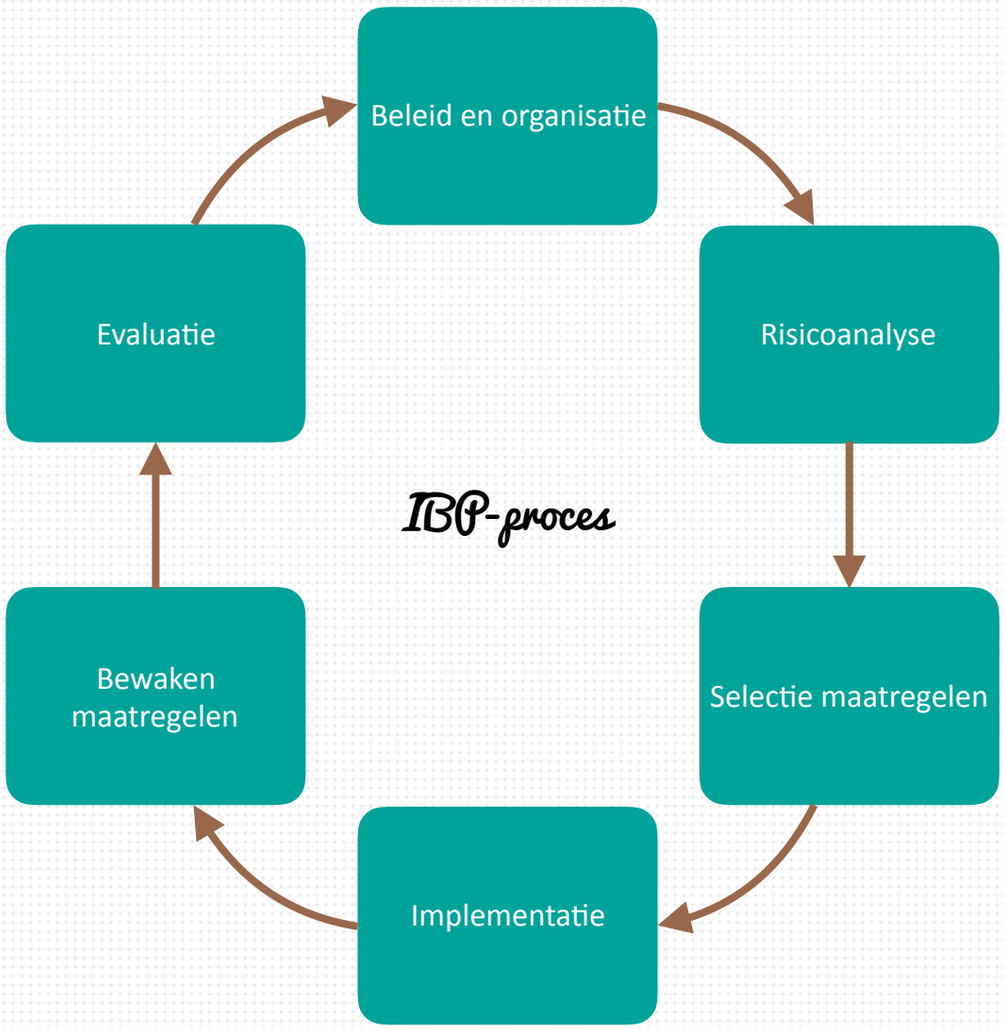
Via vakkundige aanvals- c.q. onderzoeksmethodieken zullen Certified Ethical Hackers de systemen testen. Op deze manier komen de kwetsbaarheden van de systemen boven en kunnen we die onderzoeken. Samen kunnen we de doelobjecten aangeven zodat er gericht getest wordt. Dit wordt in afstemming gedaan met de doelstellingen die voorafgaand aan de test geformuleerd zijn. De tests worden op gestandaardiseerde wijze uitgevoerd. Dit maakt dat de tests herhaalbaar zijn en resultaten door de tijd heen met elkaar vergeleken kunnen worden.

Snel inzicht in de status van de beveiliging van de systemen

De hackers werken de verkregen bevindingen en statusinformatie uit, waarbij ze ook ingaan op de zaken die wel goed gingen. De bevindingen worden samengevat in een statusrapport met daarin conclusies en aanbevelingen. Het rapport is vervolgens een goed vertrekpunt voor een verbetertraject voor het beveiligen van applicaties en systemen.



Inbedden: IBP-proces



IBP is een onderwerp dat speelt op diverse plekken in de organisatie en dus om een divers pakket aan maatregelen vraagt. Het is van belang om het onderwerp in samenhang op te pakken: want aan de ene kant goed beveiligen terwijl aan de andere kant de deur open staat, levert geen winst op.

Of je nu met Hutspot en LBVD aan de gang bent gegaan met bewustwording, een risicoanalyse of systeemtest, of zelf stappen hebt gezet, wij helpen bij het inbedden van IBP in de organisatie. Dat kunnen we doen door het maken van een samenhangend plan voor de vervolgstappen én door het structureel borgen van het IBP-proces.

Een plan van aanpak voor het vervolg

We kijken naar zaken die op langere termijn om aandacht en uitwerking vragen. We zetten samen een aanpak neer waarin duidelijk wordt wat op welke wijze en door wie wordt opgepakt en hoe het langetermijnplan voor de organisatie eruit ziet. Dit geeft houvast en zorgt ervoor dat de organisatie kan doorpakken op IBP. De aanpak op de langere termijn gaat over het organiseren van informatiebeveiliging middels de PDCA-cyclus. Hierbij gebruiken we materiaal uit het IBP Normenkader mbo.

hutspot
LBVD

Borgen van het IBP-proces in de organisatie

Een belangrijke voorwaarde voor het borgen van het IBP-proces binnen de school is de bestuurlijke agendering, opdrachtgeverschap en de omvang van de inspanning (effort) die beschikbaar wordt gesteld voor de realisatie van maatregelen. Om dit te bewerkstelligen is het wenselijk om het onderwerp formeel te beleggen binnen de organisatie. Zo borgen we het organisatorisch. Met een duidelijke opdrachtgever en de uitvoering bijvoorbeeld belegd in de rol van een Security Manager en/of een Functionaris Gegevensbescherming. Het is aan de school om te bepalen of dit als een functie of rol wordt gezien. Wij helpen de school bij het verkennen van de juiste borging in de organisatie en bij het invullen van de taken en verantwoordelijkheden van deze functies/ rollen.

IBP-proces zichtbaar maken en monitoren

De IBP monitor is een instrument om het IBP-proces in de organisatie te borgen. Voor de IBP-monitor wordt gebruik gemaakt van de statements uit het bestaande framework van saMBO-ICT. In de IBP-monitor staan alle IBP statements in één overzicht en heb je zicht op het huidige en gewenste volwassenheidsniveau van de organisatie. Op deze manier weet je welke stappen nog gezet moeten worden en kun je sturing geven aan IBP.

De IBP-monitor biedt handvatten om concrete statementplannen te maken. Op deze manier helpen wij de organisatie om op een projectmatige manier naar het gewenste volwassenheidsniveau te komen.

Extra mankracht voor realisatie van maatregelen

Heb je als school grip op IBP, dan komt het aan op het realiseren van de aanpak en de daarin opgenomen maatregelen. Heb je (tijdelijk) niet de benodigde capaciteit en/of de kennis om de uitdagingen het hoofd te bieden, dan kunnen wij daarbij helpen.

Wij hebben ervaren adviseurs en projectleiders, werken pragmatisch en effectief en het liefst vanuit een resultaatverplichting. Samen bekijken we wat de vraag is en aan welke expertise er behoefte is. Je krijgt de juiste mensen, passend bij de vraag: Hutspotters, LBVD'ers én mensen waarmee we graag samenwerken uit ons netwerk.

hutspot

LBVD

Werk waar we trots op zijn

Een fundament voor IBP bij het Wellantcollege

Wellantcollege wilde aan de slag met informatiebeveiliging en privacy en heeft Hutspot en LBVD gevraagd om de rol van kwartiermaker IBP te vervullen. Het doel was om het onderwerp in de organisatie levend te maken, op de agenda te krijgen, inzicht te bieden in de risico's die spelen én om het onderwerp in te bedden in de organisatie.

Hutspot en LBVD hebben als antwoord op deze vraag een aanpak waarmee stappen worden gezet; daarmee is een fundament gelegd voor IBP in de organisatie. Er is gestart met een informatiecampagne voor de bewustwording van medewerkers. Vervolgens is er een risicoanalyse uitgevoerd om de risico's voor de eigen organisatie in beeld te krijgen. De risico's gaven inzicht in de maatregelen die op korte termijn en met beperkte inzet konden worden gerealiseerd. Hutspot en LBVD hebben bijgedragen aan het realiseren van deze quick-wins. Voor de langere termijn is een vervolgaanpak geformuleerd aan de hand van de PDCA-cyclus.

Voor Wellantcollege is in zes maanden tijd een fundament neergelegd voor IBP binnen de school.

Lees meer over dit project op onze website: hutspot.nl/cases/

IBP-monitor en maatwerk awareness programma bij ROC van Amsterdam

ROC van Amsterdam wilde IBP naar een volgend volwassenheidsniveau brengen en een hoogstaand awareness programma aanbieden en heeft LBVD gevraagd daarbij te ondersteunen in de rol van Kwartiermaker IBP.

Om IBP naar een hoger niveau te brengen is belangrijk exact in kaart te brengen waar je nu staat (IST) en waar je naartoe wilt (SOLL). Om dit inzichtelijk te maken is de IBP monitor ontwikkeld. In één monitor is inzichtelijk gemaakt welke IBP statements wel of nog niet op het gewenste volwassenheidsniveau zijn. Een nuttig instrument waarbij je met één druk op de knop je evidence per statement in beeld krijgt. De IBP-monitor is een goed uitgangspunt om verbetermaatregelen te benoemen.

Het allerbelangrijkste is awareness. Daarom heeft het ROC van Amsterdam besloten dat awareness in 2017 extra aandacht krijgt. Hierbij vindt intensieve samenwerking met de afdeling Communicatie plaats. Om de verschillende college's zelf de regie te geven is er een awareness programma ontwikkeld dat bestaat uit 11 onderdelen. Elk college bepaalt zelf welke onderdelen zij inzetten op hun college, maatwerk dus! Vanuit de college's is deze maatwerkaanpak positief ontvangen. Dit verhoogt het draagvlak en de betrokkenheid.

hutspot

LBVD

ADEPT! bij Alfa-college

Begin 2015 is LBVD bij Alfa-college gestart met het ADEPT! programma. Een awareness-programma bestaande uit phishing, mystery guest, roadshows en kennistoets. Een divers programma wat als pilot in één jaar voor de grootste locatie succesvol is volbracht. In 2016 is LBVD gestart met het uitrollen van het programma op de andere locaties van Alfa-college.

Voor Alfa-college was er een aantoonbare toename in de bewustwording bij de medewerkers! Phishing e-mails werden beter herkend, de resultaten van kennistoets namen toe en de bevindingen van de mystery guest namen af. Elk onderdeel van ADEPT! wordt afgerond met een bevindingenrapport wat handvatten biedt voor concrete verbeteracties.

De RISMAN-methode voor risicoanalyses

Binnen Hutspot is er jarenlange ervaring met het doen van risicoanalyses volgens de bewezen RISMAN-methode. De RISMAN-methode bestaat uit vier onderdelen: het vaststellen van het doel, het in kaart brengen van de risico's, het vaststellen van de belangrijkste risico's en tenslotte het in kaart brengen van de (beheers)maatregelen. De organisatie of het project waarvoor risico's in kaart worden gebracht, wordt beschouwd vanuit verschillende invalshoeken, zodat een integraal risicobeeld wordt verkregen.

Hutspot heeft de RISMAN-methode onder andere ingezet bij:

- de transitie van het kenniscentrum Calibris naar de nieuwe Samenwerkingsorganisatie Beroepsonderwijs Bedrijfsleven (SBB) met als doel het proces goed te kunnen beheersen, de juiste maatregelen te kunnen treffen om het doel (een leeg kenniscentrum doordat medewerkers van werk naar werk zijn geholpen) te vergroten.
- de doorontwikkeling van een grote ICT-applicatie in de mbo-sector (BRON) met als doel om de grootste risico's in kaart te brengen die kunnen leiden tot het niet op tijd aanleveren van gegevens door scholen aan DUO. Met deze risico's in beeld zijn maatregelen geformuleerd om eventuele nadelige gevolgen te beperken.

Interesse in deze methodiek? ***Risicomanagement voor projecten, de RISMAN methode toegepast***, door Daniëlla van Well-Stam en Suzanne van Kinderen.

hutspot

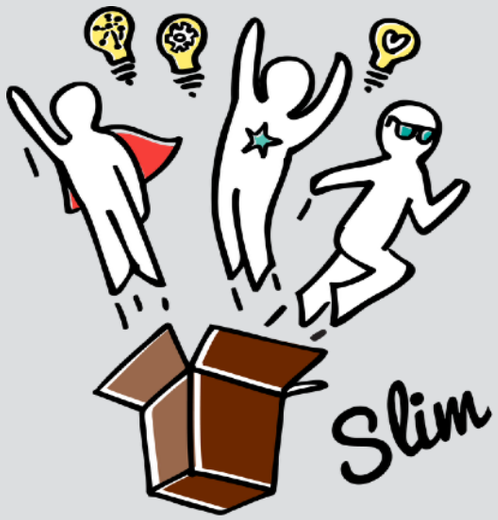
LBVD

hutspot

LBVD

Hoe wij werken

Ieder traject brengen we van visie tot resultaat. Vasthouden aan de uitgezette koers, daar scherp in zijn en pas weg gaan als staat wat afgesproken is.



Projecten gaan we aan met een slim stel mensen, echte outside of the box denkers, die hun eigen expertise inbrengen. Vaak met slimme ICT- ondersteuning en altijd met oog voor mens, techniek en organisatie.

We zien het belang van goede communicatie en werkvormen bij de acceptatie van de boodschap. Daarom werken we met creatieve partners samen om treffende oplossingen met impact te maken.

hutspot

LBVD

Vragen, opmerkingen of behoefte aan een toelichting?

Patricia:
pvanschaik@lbvd.nl of 06-30136480

Tom:
tom@hutspot.nl of 06-20491381

Rein:
rdevries@lbvd.nl of 06-30949240

Eline:
eline@hutspot.nl of 06-11355877

Rahil:
rmoentadj@lbvd.nl of 06-28915255

Elsa:
elsa@hutspot.nl of 06-23263718