Check Security

Check Privacy

HOE START IK MET HET NORMENKADER ?

VERTROUWD VEILIG SAMEN

SLBDIENSTEN.NL

HOE START IK MET HET NORMENKADER ?

- Even voorstellen
- Waarom doen we het ?
- Normenkader oude stijl
- Hoe betrek en overtuig ik mijn bestuurder?
- Nulmeting, wat houd het precies in ?
- Sneakpeak Normenkader 2024
- Enkele Tips

Check Privacy

SLBDIENSTEN.NL

EVEN VOORSTELLEN

- Rob Tesselaar
- 32 jaar actief in ICT
- Laatste 6 jaar als interim manager
  - Directeur ICT bij Porteum Lelystad (2021-23)
- Directeur Check Privacy & Check Security (2023)
- Focus op Onderwijs

SLBDIENSTEN.NL

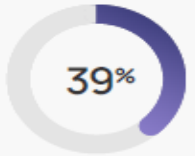
WAAROM DOEN WE HET?

1 op de 2

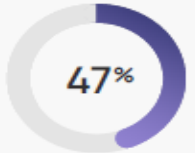
organisaties heeft in de afgelopen 3 jaar een succesvolle cyberaanval meegemaakt.

8 op de 10

zeggen dat de beveiliging van hun organisaties in toenemende mate **afhankelijk is van de beveiliging van hun partners en leveranciers.**



Bij succesvolle aanvallen met ransomware heeft **meer dan een derde van de bedrijven** losgeld betaald.



Van de kleinere bedrijven was **bijna de helft** genoodzaakt te betalen.

Top 3 van tactieken bij succesvolle aanvallen:

1. Malware
2. Phishing
3. Ransomware

Top 3 van aangevallen afdelingen:

1. IT
2. Financieel
3. Beveiliging

Digital Natives

↗ 65%

vaker op phishing-e-mails dan oudere gebruikers.

Check Privacy

SLBDIENSTEN.NL

UIT DE PRAKTIJK

Gehackt en gegijzeld: hoe MediaMarkt onderhandelde met ransomwarecriminelen

19-03-2022 14:02 Laatste update: 21:21

Daniël Verlaan

Mediamarkt werd eind vorig jaar slachtoffer van een grote ransomware-aanval. Er werd twee weken lang onderhandeld met de criminelen. RTL Nieuws wist toegang te krijgen tot stevige onderhandelingen die bijna altijd geheim blijven.

Ransomware heeft een steeds grotere impact op onze maatschappij, maar er is maar weinig bekend over hoe deze cybercriminelen te werk gaan, hun werkzaamheden professionaliseren en slachtoffers onder druk zetten.

RTL Nieuws geeft voor het eerst een exclusief kijkje achter de schermen:

Computers gegijzeld

Het is maandag 8 november 2021 als de computers van de MediaMarkt opeens op slot gaan. Het bedrijf vraagt werknemers om de gegijzelde systemen te mijden en alleen maar producten te verkopen die fysiek in de winkel staan. Het afhalen en retourneren van producten is niet meer mogelijk.

De criminele hackers hebben een volgens de MediaMarkt 'zeer gerichte' aanval op de systemen uitgevoerd, waarbij er op grote schaal Windows-systemen zijn gegijzeld. Het gaat om de computers van de Europese vestigingen, waaronder 49 winkels in Nederland.

NOS Voetbal • Dinsdag 12 september, 09:09

KNVB betaalt losgeld aan hackers om vertrouwelijke gegevens te beschermen

De KNVB heeft losgeld betaald aan cybercriminelen die in april persoonsgegevens hebben gestolen van de voetbalbond. De hackersgroep LockBit gebruikte hierbij gijzelsoftware. Volgens RTL Nieuws was de eis ruim 1 miljoen euro. De KNVB wil niet zeggen om hoeveel geld het gaat.

De KNVB deelt het nieuws in een advertentie in twee landelijke kranten en in een bericht, waarin ze mensen waarschuwen dat hun gegevens mogelijk in handen zijn van die criminelen. De bond zegt het betalen van losgeld een moeilijke keuze was, maar dat er uiteindelijk "onder deskundige begeleiding afspraken" met de hackers zijn gemaakt. De bond is er nog niet helemaal gerust op dat de criminelen na het krijgen van het losgeld de gegevens ook echt niet zullen verspreiden en roept mogelijke gedupeerden op om extra alert te blijven op misbruik van hun gegevens.


«ADVERTENTIE»

MEDEDELING DATALEK KNVB

Cybervеiligheid

Een zwak wachtwoord legde de gemeente Hof van Twente plat

Dat de gemeente Hof van Twente eind vorig jaar te maken kreeg met ransomware, had voorkomen kunnen worden. Er werd een aantal klassieke fouten gemaakt.

Kristel van Teeffelen 16 maart 2021, 15:39

De aanval met gijzelsoftware bij de gemeente Hof van Twente was het gevolg van een zwak wachtwoord. Dat de criminelen er vervolgens in slaagden een groot deel van de gemeente plat te leggen, kwam door eerder gemaakte fouten bij de inrichting van de systemen.

Dinsdag presenteerde de gemeente verschillende onderzoeksrapporten over wat betrokkenen zelf 'een crisis' noemen. Die crisis begon op 1 december vorig jaar, toen bleek dat Hof van Twente getroffen was door ransomware. De aanvallers versleutelden bestanden, waardoor de gemeente er zelf niet meer bij kon. De dienstverlening aan burgers viel stil.

De hackers lieten een boodschap achter, die ook uit verschillende printers op het gemeentehuis rolde: wil je je bestanden terug, neem dan contact op via dit mailadres. Via *de Volkskrant* lekte uit dat de aanvallers 750.000 euro in bitcoin eisten in ruil voor de sleutel. Een opvallend hoog bedrag vergeleken met andere bekende gevallen van ransomware.

Het wachtwoord werd veranderd in Welkom2020

De specialisten die in opdracht van de gemeente onderzoek deden, komen tot de conclusie dat de aanval voorkomen had kunnen worden. Zo wijst het cybersecuritybedrijf NFIR op een server van de gemeente, die sinds oktober 2019 toegankelijk was via internet. Sindsdien werden miljoenen pogingen gedaan om via deze poort binnen te komen. Vreemd is dat niet, zegt Arwi van der Sluijs van NFIR. "Elk netwerk heeft hiermee te maken. Poorten worden gescand door het hackersgilde, maar bijvoorbeeld ook door valide dienstverleners."

Ook back-up aangetast

Bol.com heeft 750.000 euro overgemaakt op een rekening van oplichters, terwijl de webwinkel in de veronderstelling was Brabantia te betalen. De Brabantse fabrikant van huishoudelijke artikelen heeft alsnog recht op het geld, meldt *Het Financieele Dagblad* (FD) zondag op basis van een uitspraak van de rechter in april.

Top bleef geld storten

Pathé opgelicht: nepmails kosten bioscoopketen 19 miljoen

10 november 2018 11:25 • Aangepast 10 november 2018 13:59

Bioscoopketen Pathé is voor ruim 19 miljoen euro opgelicht. De top van het bedrijf kreeg mails van oplichters die zich voordeden als een topbestuurder. Ondanks twijfels van twee topmensen hierover, konden de fraudeurs toch 19 miljoen euro buitmaken.

Dat blijkt uit een uitspraak van de Amsterdamse kantonrechter van eind oktober, die gisteren is gepubliceerd. Een fraudeursbende meldde zich op 8 maart bij topvrouw Dertje Meijer en financieel directeur Edwin Slutter, via een nepmailadres als bestuurder van het Franse hoofdkantoor.

Check Privacy

SLBDIENSTEN.NL

OF DICHTER BIJ HUIS..

NOS Nieuws Sport Live Programma's

NOS Nieuws • Zaterdag 13 april, 13:44

Schoolboekenleverancier Iddink gehackt, mogelijk klantengegevens gelekt

Iddink, een organisatie die schoolboeken en digitaal lesmateriaal verkoopt, is getroffen door een aanval met gijzelsoftware. Dat heeft de organisatie zelf bekendgemaakt.

Gijzelsoftware

Universiteit Maastricht na cyberaanval: 'Blijf van computers af'

Het college is in ieder geval nog tot en met maandag dicht, maar hoopt de systemen dinsdag weer draaiende te krijgen. Scholieren krijgen nieuwe inloggegevens.

Het is niet duidelijk hoeveel geld er is betaald om de toegang tot de bestanden terug te krijgen.

Bij een ransomware aanval op de Universiteit van Maastricht in 2019 werd twee ton aan losgeld betaald. Vaak weigeren slachtoffers ook te betalen, zoals de gemeente Hof van Twente.

SLBdiensten / Nieuws overzicht / Claim van €2 miljoen aan dataverbruik waarschuwt ...

Claim van €2 miljoen aan dataverbruik waarschuwt onderwijsinstellingen voor gevaren cryptojacking (video)

27 februari 2024

Check Privacy

SLBDIENSTEN.NL

HET GEVEN VAN GOED ONDERWIJS LOOPT GEVAAR

- Het leveren van je belangrijkste product loopt gevaar
- De veiligheid van medewerkers en leerlingen kan in het geding zijn
  - Gegevens van hen kunnen voor andere doeleinden worden gebruikt!

- Als (onderwijs)organisatie heb je de verantwoordelijkheid:
  - Om je bedrijfsvoering (dus ook IBP) goed op orde te hebben
  - Ervoor te zorgen dat je medewerkers en leerlingen zo goed mogelijk begeleid naar digitaal veilige bewustwording.

HET NORMENKADER IS ER NIET VOOR NIETS!

Check Privacy

SLBDIENSTEN.NL

NORMENKADER (OUDE STIJL)

- Normenkader IB (April 2023) ⟶ P in juni 2024
  - 15 domeinen rondom informatiebeveiliging
  - 69 bijbehorende normen
  - P heeft 25 bijbehorende normen

  - Elke norm heeft een toetsingskader. Dit beschrijft het minimum niveau
  - Voorbeeldmaatregelen toegevoegd, dit maakt het concreter
  - Eind 2027 moeten alle scholen op Niveau 3 (gedefinieerd) zitten
  - Inspectie neemt normenkader mee in haar beleid

ENKELE UITSPRAKEN VANUIT DE PRAKTIJK..

- “Oh… 2027? Maar dat is nog ver weg joh!“
- “De overheid vraagt wel, maar levert niet”
- “Daar heb ik toch geen verstand van?!”
- “Dat kost mij een extra FTE, die ik niet kan inzetten in het onderwijs”

HOE BETREK EN OVERTUIG IK MIJN BESTUURDER?

- Ga in gesprek over de meest prangende uitdagingen:
  - Bewustwording, Expertise & Capaciteit
- Overtuig dat werken aan bewustwording hand in hand kan gaan met verzorgen van goed onderwijs,
  - Namelijk door het in te bedden in je onderwijs

- Ga in gesprek over welke risico's centraal staan. Maak het concreet, behapbaar en begrijpelijk.
  - Centraal staat : "Hoe verminder je de bestaande risico's? "
  - Maak gebruik van een nulmeting om te laten zien waar de organisatie staat.

En dan nu in gesprek !

SLBDIENSTEN.NL

NULMETING: WAT HOUD HET PRECIES IN ?

- Waar staat de organisatie t.o.v. het normenkader ?

  - Kennismaking & uitleg proces
  - Diverse interviews met directe betrokkenen a.d.h. Checklist
    - Centrale vraag : “Wat is er aan beleid” ?
  - Korte review situatie IT
  - Korte scan op contractmanagement (in kaart brengen risico’s)
    - Speciale aandacht voor domein 15 (Ketenbeheer)
  - Rapportage & evaluatie

EINDRAPPORTAGE, WAT NU ?

- Graadmeter waar organisatie staat
- Identificatie van kwetsbaarheden en potentiële risico's.
- Een gedetailleerd rapport met actiepunten voor de organisatie

SNEAKPEAK NIEUWE NORMENKADER (JUN 2024)

Check Privacy

Een nieuw Normenkader? Nou ja nieuw.. Vooral Beter!

Wat is er anders ?

- Alles staat op 1 plek
- Normen zijn concreter geformuleerd
- Er zijn voorbeeldmaatregelen & gerelateerde wetten per norm
- Nu ook normen voor Privacy !
  - 7 domeinen
  - 25 normen

SLBDIENSTEN.NL

SNEAKPEAK NIEUWE NORMENKADER (JUN 2024)

Check Privacy

- Nieuwe indeling van de volwassenheidsniveau's
  - 1. = Ad Hoc (was Initieel)
  - 2. = Herhaalbaar
  - 3. = Bepaald* (was gedefinieerd)
  - 4. = Beheerst (was beheerst en meetbaar)
  - 5. = Continu verbeteren
- De voorbeeldmaatregelen maken het mogelijk om nog meer gericht en projectmatig te werken!
- Stap voor stap toewerken naar het gewenste niveau..

Maar eerst die nulmeting!

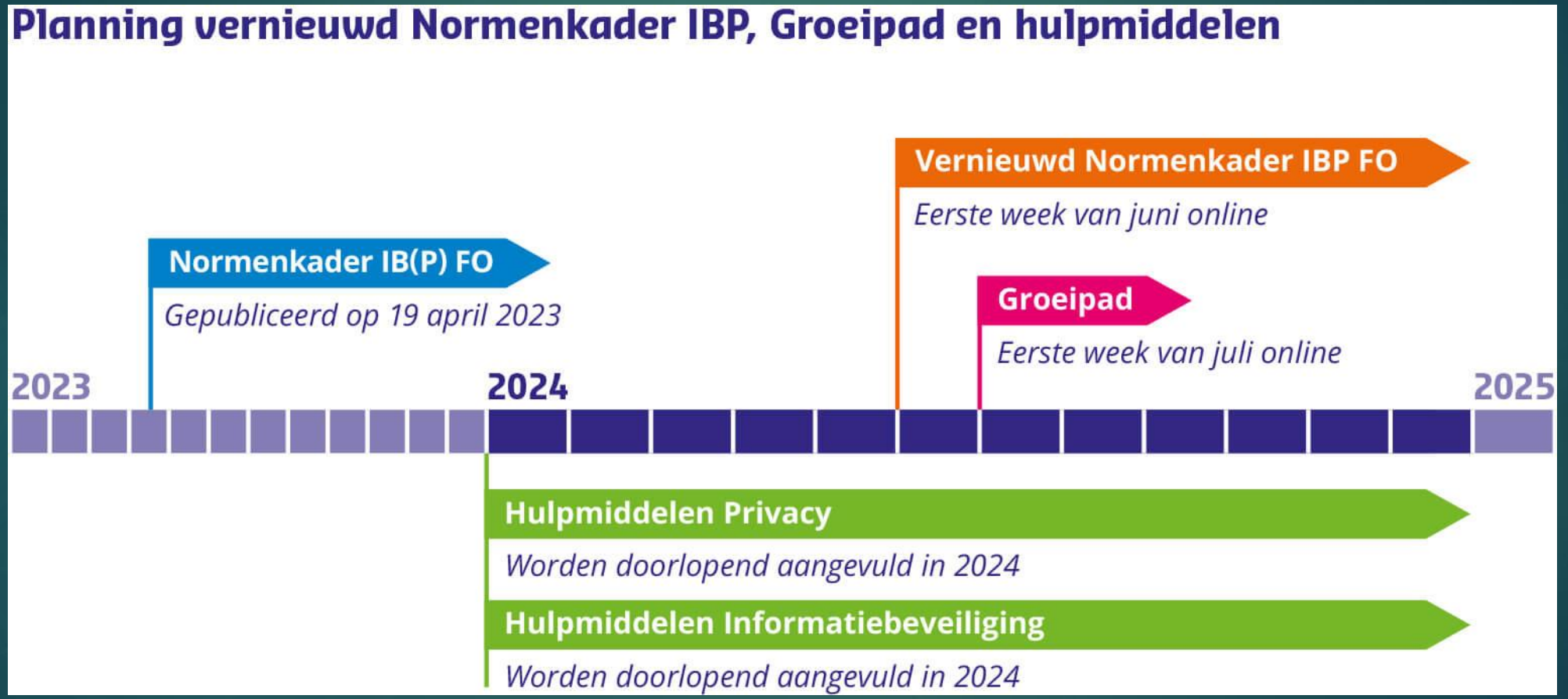
* minimum eind 2027

SLBDIENSTEN.NL

GROEIPAD

- Het Groeipad vervangt de tabel over het aan de slag gaan met het normenkader in de huidige kennisnet-pdf (blz. 94).
- Wegwijzer om stapsgewijs de digitale veiligheid in jouw school op orde te brengen.
- Afhankelijk van waar jouw school staat, kun je instappen in het Groeipad.

PLANNING



SAMENVATTING

- Normenkader IB (April 2023) → Herijking in juni 2024
  - 15 domeinen rondom informatiebeveiliging & 69 bijbehorende normen
- Normenkader P in juni 2024
  - Heeft 7 domeinen & 25 bijbehorende normen

- Er zijn voorbeeldmaatregelen & gerelateerde wetten per norm
- Er komt in juli een groeipad i.p.v. de eerdere fasering (maakt het concreter)

- Eind 2027 moeten alle scholen op Niveau 3 zitten (Bepaald)
- Inspectie neemt normenkader mee in haar beleid

GEEN TIJD MAAR PRIORITEIT!

BEGIN GISTEREN EN NIET MORGEN

Check Privacy

- Er is nu nog 3,5 jaar (2024-2027)
  - 15 Domeinen & 69 normen + 25 normen "P" → Veel werk!
  - Geen afvinklijstje
- IBP is een verantwoordelijkheid van iedereen in de organisatie en met name van het MT
  - Geen ICT-feestje
  - Focus op "Bewustwording" → HRM-plan
  - Creëer een Team van belanghebbenden & betrek bestuurder/RvT
- Inbedden in (meerjaren)begroting & jaarkalenders scholen

NOG ENKELE TIPS:

- KISS! Keep it stupid simple. Stel geen onnodige teksten of documenten op waar niemand naar kijkt, of die geen nut hebben bij de implementatie van technische of organisatorische maatregelen.
- Houd het binnen proporties. Breng de documentatie en de maatregelen in lijn met de grootte van je organisatie.
- Pas reverse engineering toe. Heb je nog niet (veel) gedocumenteerd, maar gelden er wel bepaalde processen, procedures of werkwijzen?
  - Start eenvoudig met het opschrijven van hoe je de dingen doet.
  - Met terugwerkende kracht kun je dan een deel van het beleid al formuleren.

ENKELE TIPS:

- Benader in gesprekken met collegá's IBP vanuit risicoperspectief.
  - Welke risico's zijn afgelopen tijd vastgesteld (uit DPIA's, risicoanalyses, incidenten)
  - Welke acties zijn er gepland op basis van deze risico's? Lukt het om deze acties uit te voeren?
  - Zijn er incidenten geweest en hoe zijn deze opgepakt? Lukte het om deze incidenten snel op te lossen?

Centraal staat : Hoe verminder je de bestaande risico's ?

IBP PLATFORM SAMENWERKENDE LEVERANCIERS

- Brug tussen de dynamische wereld van informatiebeveiliging en privacy en het funderend onderwijs
- Bundelt krachten en kennis van leveranciers die zich in het funderend onderwijs bezighouden met informatiebeveiliging en privacy
- Gesprekspartner van het Programma Digitaal Veilig Onderwijs (DVO) & SIVON

Door onze gezamenlijke expertise en kennis willen we met elkaar en het programma Digitaal Veilig Onderwijs een publiek-privaat ondersteuningsaanbod realiseren, waarmee scholen ontzorgd kunnen worden.

SLBDIENSTEN.NL

IBP PLATFORM SAMENWERKENDE LEVERANCIERS

APS IT diensten
Check Privacy
CLOUD/LIFE.
skool
SPEYK
cloudwise
de Rolf groep
DOTSAFE CYBER SECURITY EXPERTS
SLBDIENSTEN.NL
FLEXfg
heutink.ict
HOLM SECURITY
YOURSAFETYNET
ICTRECHT
ICT VOOR SCHOLEN
privacy1
PRIVACY OP SCHOOL
privacyteam
Prowise

Check Privacy

SLBDIENSTEN.NL

Check Security

Check Privacy

VRAGEN?

www.check-privacy.nl
www.check-security.nl

SLBDIENSTEN.NL