Aankondiging

Webinar Cyberweerbaarheid

donderdag 24 februari 2022

Cyberweerbaarheid in de zorg
Digitale veiligheid, hoe organiseer je het en waar moet je als zorginstelling rekening mee houden

Tijdens een eerder webinar hebben wij uitgebreid stilgestaan bij een mogelijke aanval van ransomware; wat is de impact? Hoe moet je reageren? en hoe kun je het voorkomen?
Als het gaat om de digitale weerbaarheid van organisaties zijn de berichten hierover alarmerend en urgent. De situatie is ernstig. Veel zorginstellingen lopen achter op het gebied van digitale weerbaarheid. Incidenten hebben vaak grote gevolgen, voor de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens. Maar er zijn ook grote financiële gevolgen en het imago van de organisatie kan schade oplopen. Informatiebeveiliging is van strategisch belang en het vereist blijvende aandacht.

Op 24 februari gaan wij tijdens het webinar Cyberweerbaarheid hierover in gesprek met Rens van der Logt (Infozorg), Richard Strooper en Wijnand Verweij (beide van Pinewood). Pinewood is specialist in informatiebeveiliging, levert een scala aan diensten op dit gebied, waaronder ook aan zorginstellingen, en is hiervoor aangesloten op het Zorg Detectie Netwerk. Infozorg richt zich specifiek op de zorgsector bij de advisering en ondersteuning van beheer, ontwikkeling en implementatie. Hierbij wordt o.a. gebruik gemaakt van SAAR dat ook ondersteunt bij de inrichting van informatiebeveiligingsprocessen. Infozorg en Pinewood zijn kennispartner van Stichting IP-Zorg.

Verslag

Webinar Cyberweerbaarheid

donderdag 24 februari 2022

Peter van der Zwan, voorzitter van de stichting IP-Zorg opent de bijeenkomst.
Relevantie van dit onderwerp blijkt o.a. uit een deze maand gepubliceerd IBM-rapport over ontwikkelingen in het dreigingenprofiel. In het rapport wordt verwezen naar een toename van dreigingen als gevolg van thuiswerken, maar ook door geo-politieke spanningen. In conflicten tussen landen wordt steeds meer gebruik gemaakt van cyber attacks.

Deelnemers introduceren zich kort.
Rens van der Logt geeft aan dat er bij Infozorg veel kennis is van functioneel beheer; Infozorg ondersteunt zorgorganisaties bij de inrichting en beheer van de zorgapplicaties. Daarnaast is de ervaring met informatiebeveiliging binnen Infozorg behulpzaam bij de projecten.

Wijnand Verweij is accountmanager bij Pinewood met de focus op de zorgsector. Pinewood, opgericht in 1994, gestart in de netwerkbeveiliging en in de loop der jaren uitgegroeid tot specialist informatiebeveiliging; met naast de technische kant ook aandacht voor de beleidsmatige kant. In Delft staat het Security Operation Center (SOC). Speerpunt van Pinewood is het monitoren van de ict-infrastructuur van klanten.
Richard Strooper zit als CTO bij Pinewood op het raakvlak beleid en techniek; Richard is veel werkzaam in de zorgsector.

Peter vraagt de deelnemers welke ontwikkelingen ze zien op het gebied van informatiebeveiliging.
Pinewood ziet dat steeds meer gebruik wordt gemaakt van cloudleveranciers; klanten komen met vragen over veiligheid van SAASoplossingen. Er wordt steeds meer thuisgewerkt en er is een toename van ransomware, phising, e.d. Ook is er steeds meer aandacht voor de NEN 7510.

Peter merkt dat op dat je bij zorgorganisaties die gebruik maken van cloudoplossingen vaak hoort dat ze geen zorgen hebben over informatieveiligheid omdat de clouddienstverlener dat regelt. Maar bij het uitbesteden van de techniek moet de klant *ook* securityeisen stellen én controleren! De klant blijft verantwoordelijk. De klant vraagt daarom vaak aan Pinewood om een soort van audit uit te voeren.

Ook Infozorg ziet steeds meer SAASapplicaties, vooral in combinatie met SSO-oplossingen. Men wil immers voorkomen dat medewerkers steeds opnieuw moeten inloggen, wanneer gebruik wordt gemaakt van meerdere SAASapplicaties. Daarnaast een toename van bewustwording voor vertrouwelijkheid van data. Extra inzet training en aanscherping beleid.

10:00
Inrichting SSO-oplossing bij meerdere leveranciers
Juist wanneer organisaties steeds meer gebruik maken van cloudoplossingen (SAAS), is het van belang goed na te denken over de toegang tot deze applicaties. Immers, niet alleen moet worden voorkomen dat medewerkers steeds opnieuw per toepassing moeten inloggen, maar ook is het van belang dat het toegangsbeheer goed wordt ingericht en bij voorkeur centraal wordt beheerd. Vaak wordt gebruik gemaakt van Azure AD als centrale authenticatievoorziening, waarbij ook een koppeling met het personeelssysteem wordt gerealiseerd. Het borgt bijvoorbeeld dat wanneer medewerkers de organisatie verlaten, toegang tot de verschillende applicaties wordt geblokkeerd.
Ook wanneer gebruik wordt gemaakt van cloud toepassingen, dient access control goed te zijn ingericht. Denk dus aan dingen als condition access; kijk naar *wat* die persoon is, *wie* is die persoon en

waar komt die persoon vandaan; met andere woorden: *welke rol vervult de betreffende persoon en voor welke organisatie-eenheid heeft hij rechten nodig.* De toegenomen kwetsbaarheid heeft overigens niet alleen te maken met het feit dat meer in de cloud wordt gewerkt, maar ook sprake is van een grotere verscheidenheid aan (mobiele) devices waarmee toegang wordt verkregen en de verschillende internet-of-things. Deze krijgen vanaf verschillende locaties toegang tot het bedrijfsnetwerk en kunnen niet op voorhand worden vertrouwd. Organisaties dienen daarom het zero-trust concept als basis voor hun beveiliging te kiezen (niets is op voorhand vertrouwd).

Vroeger was een locatie met wat daar gebeurde veilig; nu ga je ervan uit dan mensen vanaf allerlei locaties kunnen inloggen en moet je er van uit gaan dat dat op voorhand *niet veilig* is. . .

13:00
Vraag aan Rens: hoe ga je vanuit functioneel beheer hiermee om?
Zorgorganisaties zijn zich bewust van vertrouwelijke data, maar het inzicht in welke applicaties en in welke koppelingen ze aanwezig zijn wordt niet altijd op 1 plek beheerd. En ook nog eens vanuit verschillende invalshoeken; bijvoorbeeld ook vanuit een managementsysteem voor informatiebeveiliging. Het is lastig verschillende documentaties overzichtelijk te houden. Dus maak ook je ISMS een integraal onderdeel van je informatiehuishoudingssyteem. Je moet weten welke data je verwerkt (AVG), om zo je risico's te documenteren, verantwoordelijkheid inzichtelijk maken en te koppelen aan de beheersnormen van de NEN 7510.

15:00
Organisaties kiezen vaak ook voor een (centrale) authenticatievoorziening voor een cloudoplossing; in de zorg wordt Azure AD vaak gekozen. Hiermee wordt ook invulling gegeven aan de single-sign-on. Aandachtspunt is wel de aankomende Wet Digitale Overheid. Deze wet zal naar verwachting dit jaar in werking treden en betekent dat de portalen voor clienten die zorginstellingen bieden, toegankelijk moeten zijn via de wettelijk erkende (Europese) inlogmiddelen (zoals DigID). Voor veel zorginstellijngen betekent dit nog een transitie die ze moeten uitvoeren.

16:35
Wat wordt verstaan onder Cyberweerbaarheid?
Preventieve maatregelen zoals een firewallbescherming en anti-virussoftware zijn altijd wel getroffen; wat vaak nog niet duidelijk is welke risico's je daarmee hebt afgedekt. Ga eerst na welke risico's je wilt afdekken en bepaal dan je maatregelen, ook de detectieve en correctieve maatregelen zijn van belang (denk aan continue monitoring van je bedrijfsnetwerk)! *Cyberweerbaarheid is een samenspel tussen risico's en samenhangende maatregelen*. Wat je vaak ziet is dat maatregelen technisch ok zijn, maar dat beleid en beveiligingsplannen als losse documenten zijn gemaakt, niet helder samengevoegd in een proces dat volgens de pdca-cyclus kan worden gevolgd. Hiervoor wordt vaak ondersteuning gevraagd.

Maar 100% veiligheid bestaat niet! Dat zou een onwerkbare situatie creëren. Daarnaast is de zorg inherent aan een open cultuur; de zorg staat voorop en de security mag niet al te beperkend zijn. Goede afweging nodig. En als er wat gebeurt moet het mogelijk zijn tijdig te reageren om de schade zoveel mogelijk te beperken.

20:30
Hoe gaan zorgorganisaties om met risico's?
In de zorg heb je vaak capaciteitsproblemen en wordt veel gewerkt met uitzendkrachten. Ook die moeten in een cliëntendossier kunnen kijken. Daarvoor moet je beheersbare afspraken maken en controleren. De technische kennis is wel aanwezig maar de controleslag ontbreekt vaak. Organisaties worden geconfronteerd met nieuwe ontwikkelingen en vooral nieuwe kwetsbaarheden. Ze moeten daarin keuzes maken op basis van de gevoeligheid van informatie; zoals processen uitschakelen of

risico accepteren? En weer de controleslag waarmee je ook duidelijk kunt maken dat maatregelen niet meer werken en dus niet nodig zijn. Het beveiligingsbewustzijn van medewerkers wordt steeds beter maar voorkom overbodige maatregelen. Met technische maatregelen alleen ben je er niet; de mens blijft de zwakke schakel in de beveiliging.
Peter wijst in dit verband op de wegwijzer *Informatieveilig gedrag in de zorg*; een initiatief van VWS en brancheorganisaties Zorg; vanaf 1 april belegd bij ECP in het programma Digivaardig in de zorg.

24:00
Naar aanleiding van een chatvraag of inzage in dossiers goed wordt gelogd.
Met andere woorden, heb je een afspraak of is er een proces waarin je kunt nagaan of de toegang tot het dossier juist verloopt. Je kunt bijvoorbeeld periodiek standaard checks doen. Bij Pinewood komen verzoeken binnen om toegang tot ecd's te monitoren. Resultaten realtime te filteren en een alarmering doen op verdachte benaderingen. Filtering rules worden met de klant opgesteld. Monitoring initieert reactive maatregelen en bevordert awareness. Medewerkers weten dat activiteiten worden gemonitord.

31:00
Security-by-design; hoe gaat een zorgorganisatie daarmee om bij aanschaf van software?
In de eerste plaats beleidsmatig vastleggen waaraan leveranciers moeten voldoen en dat ook toetsen. En ga periodiek met leveranciers in overleg; naast certificaat NEN 7510 kun je vragen naar pentesten vragen of pentesten laten uitvoeren.
Hou een overzicht bij van je leveranciers. A.g.v. acute kwestbaarheid moet je bij je leveranciers terecht kunnen; hou ook bij hoe snel ze reageren. Leveranciersmanagement wordt steeds belangrijker en moet een onderdeel zijn van risicomanagement.
Wat je normaliter doet in je eigen infrastructuur moet nu de leverancier doen. Zorg vooraf voor goede contracten en bewerkersovereenkomsten.
Let vooral op bij koppelingen naar 'achterliggende' leveranciers in de keten; ga ook na of voor je vaste leveranciers de toeleveranciers in beeld zijn. In het eerdergenoemde rapport van IBM wordt dit ook als toenemend risico genoemd.

Leverancierssketens zijn een toenemende kwetsbaarheid; klanten zijn verplicht bij leveranciers door te vragen naar de toeleveranciers.

41:00
Relatie Z-Cert en SOC
Zoals eerder aangegeven is een continue monitoring van het ICTnetwerk van groot belang; immers, bedrijfsnetwerken zijn vrijwel altijd gekoppeld aan het internet; dit betekent dat ze per definitie doorlopend door kwaadwillenden worden gescand op kwetsbaarheden die misschien de mogelijkheid bieden om in te breken op het bedrijfsnetwerk. Om schade te beperken is het allereerst van belang het netwerk in te delen in verschillende zones en de koppeling met internet via een DMZ (de-militarized zone) te laten lopen. Maar het netwerk continu bewaken met behulp van een intrusion detection en prevention systeem (IDS IPS) is van toenemend belang om bijvoorbeeld een ransomware aanval te voorkomen. Deze continue bewaking vindt plaats vanuit een zogenaamd Security Operations Center (SOC). Probleem is echter dat voor veel zorginstellingen het niet mogelijk is om hier 7x24 uur monitoring op uit te laten voeren door een SOC, hetgeen zowel met beschikbaarheid als met de hiervoor benodigde specialistische expertise te maken heeft. Veel zorginstellingen kiezen er daarom voor gebruik te maken van een SOC-dienstverlener zoals Pinewood.

Het SOC van Pinewood legt voor elke klant een log-collector aan die de logfiles van de verschillende applicaties verzamelt. Dit wordt gemapt met Z-Cert meldingen; 'matches' worden teruggekoppeld naar de klant.

Bij het Pinewood SOC worden vanuit een centrale post alle klantensystemen gemonitoord; monitoring is per klant ingesteld voor de klantspecifieke situaties / risico's.

44:00
n.a.v. chat: leeesbaarheid security rapportages
Het is een algemeen probleem dat bij klanten vaak de kennis ontbreekt om securityrapporten (pentesten, security scans) te interpreteren. Belangrijk is dat je partijen om je een hebt die de vertaling naar jouw situatie kan maken. En advies uitbrengen wat je ermee doet; niet alleen technisch, ook procesmatig.

47:00
Infozorg & Saar
Infozorg maakt gebruik van Saar om de informatiehuishouding bij een organisatie vast te leggen en te beheren. Dus ook je volledige ISMS als integraal onderdeel. Zie in de bijlage enkele ppt-sheets.

52:00
Specifieke kenmerken cyberweerbaarheid zorgsector?
De balans tussen 'open karakter' zorg en privacy; naast preventieve maatregelen moet dan wel extra worden geïnvesteerd in het vroegtijdig ontdekken van incidenten en de afhandeling daarvan.

Security verplaatst zich van IT naar business; IT is slechts nodig voor inrichtingszaken. Apparatuur wordt aangeschaft voor de lange termijn; dat geldt niet voor de sofware. Dat vergt aanvullende security/ controle maatregelen.

57:00
Domotica! IoT!
Alle mogelijke systemen kunnen worden gekoppeld aan internet of aan systemen.
Maak bijv. met scans inzichtelijk wat er aan je netwerk hangt zodat je het kunt beheren
Er worden op IoT-systemen wel testen uitgevoerd; maar ze zijn zeer divers en er zijn nog geen keurmerken. Ga er in beginsel van uit dat ze onveilig zijn.
Het even koppelen van een digitale camera of planbord wordt steeds gangbaarder; een extra kwetsbaarheid voor het netwerk. Pentesters hebben vaak veel succes bij printers en camera's!

62:00
Over verschillen scans
Security scan is vooral organisatorisch; faciliterend; gericht op processen
Een kwetsbaarheidsscan is een scan op zwakke plekken in je ICT-omgeving die je bijvoorbeeld maandelijks uitvoert; het signaleert bijvoorbeeld wanneer patches, security updates niet zijn uitgevoerd waardoor kwetsbaarheden kunnen worden misbruikt.
Een kwetsbaarheidsscanning vraagt resources van een organisatie; output moet worden beoordeeld en o.b.v. prioritering moeten acties volgen.
Pentest
Waar een kwetsbaarheidsscan inzicht geeft in de kwetsbaarheden van de in gebruik zijnde software, geeft een pentest bijvoorbeeld inzicht in de mate waarin de kwetsbare software ook daadwerkelijk kan worden misbruikt. Of wordt het voorkomen door een adequate scheiding tussen de verschillende zones in het netwerk dan wel verschillende maatregelen op applicatieniveau?
De pentest kijkt dus ook naar de opbouw en gebruik van de infrastructuur.

66:00
Zijn bestuurders van zorginstelling zich voldoende bewust van cyberweerbaarheid? Wordt er voldoende in geinvesteerd? Is er draagvlak?
Voorwaarde is dan wel dat de SO-rol niet is belegd binnen de ict-afdeling maar dichter bij het bestuur.

Pinewood geeft aan dat bij risicoworkshops steeds vaker andere dan ict-afdelingen worden betrokken; cyberweerbaarheid is de verantwoordelijkheid van de hele organisatie. Problemen liggen vaak niet alleen bij de ict-afdeling; die heeft meestal hun zaakjes wel op orde. Het zijn meestal de bedrijfsprocessen; de awareness waar de grootste risico's liggen.
En bestuurder niet pas betreken a.g.v. een incident

70:00
Tips FG
Zorg dat je onafhankelijk kunt functioneren; zorg ervoor dat je niet zelf bij uitvoering van security betrokken bent.
Eerst risico dan de techniek; laat risico's leidend zijn voor je maatregelen.
Houd korte lijnen met de IT-afdeling en schroom niet om een specialist in de arm te nemen als het nodig is.
Betrek zoveel mogelijk de bestuurslaag bij beslissingen
Beoordeel op vooraf vastgestelde termijnen de risico's met de bestuurders
Hou je ISMS bij zodat je altijd een overall inzicht hebt
Scherm het ISMS niet af maar laat het een intern-open document zijn.

73:00
Een deelnemer komt met enkele punten waar hij het niet mee eens is. Daar kan vanwege de slechte geluidskwaliteit niet op worden gereageerd. Gevraagd wordt zijn inbreng via chat of e-mail te stellen.

75:00
Nieuwe technologieën en platform bieden vele mogelijkheden om gegevens uit te wisselen en wordt een steeds grotere uitdaging. Denk voor dergelijke installaties van goed na over de inrichting; besteed aandacht aan autorisaties. Hou de mogelijkheden van een pakket tegen je risico's aan; bouw zo nodig beperkingen in. Security by design!

Platforms als Teams en Sharepoint zijn gericht op samenwerking maar zorg wel dat je dat goed regelt. Zelfs als je de configuratie uit handen geeft ziet Pinewood soms achteraf nog kwetsbaarheden als gevolg van foute configuraties. Documenten kunnen bijvoorbeeld hierdoor onbedoeld gedeeld worden of toegankelijk zijn voor andere organisaties

78:00
Naar aanleiding van een chatvraag over de complexe kwetsbaarheid log4j een enkele tip.
Securitytechniek is een apart vak; als je de kennis niet binnen bereik hebt schroom dan niet een specialist in te huren. Ga er niet van uit dat je dit soort zaken zelf kunt doen en regel vooraf je contacten. Als onderdeel van je incident response maatregelen.

80:00
Afronding.
Peter benadrukt nog eens enkele punten:

- de op risico's gebaseerde benadering voor beveiligingsmaatregelen,
- ervan uitgaan dat eigenlijk niets veilig is,
- awareness bij medewerkers en betrokkenheid bestuurders,
- aansluiten op beheerproces,
- dat security geen onderdeel is van de ict en moet aansluiten op het beheerproces.

82:00
Peter dankt sprekers voor hun inbreng en de deelnemers voor hun geduld om mee te luisteren.
Deelnemers krijgen een IP-Zorg mok 'met inhoud'.

OPMERKINGEN N.A.V. CHATBERICHTEN

[15:16] chat
Azure AD vaak in combinatie met bv Hello Id van Tools4Ever.
Wij zien inderdaad Hello Id bij onze klanten maar er zijn er ook genoeg die alleen Aure AD icm ADFS oplossingen gebruiken, het is een eigen voorkeur. Het belangrijkste is dat er een centraal te managen "single source of truth" is.

[15:19] chat
hoe staat het met de NEN 7510 in de VVT?
Wij zien dat de NEN 7510 steeds meer gebruikt wordt als input voor beleid en maatregelen. Betekent niet dat iedereen meteen gecertificeerd is maar het is wel *de* standaard die gebruikt wordt als houvast. Naast de NEN 7510 zijn de CIS controls ook een welkome aanvulling bij de meeste organisaties. Een dergelijk traject kost relatief resources. De verwachting is wel dat dit de komende jaren zal gaan toenemen vanwege de groeiende aandacht van de norm binnen de zorg in het algemeen.

[15:19] chat
hoe staat het met die transformatie naar DigiD? (in de VVT)
Een DigiD koppeling vraagt tevens als NEN 7510 een behoorlijke jaarlijkse audit last. Ja wij komen het tegen maar ik kan er geen duidelijk cijfer op leggen. DigiD wordt natuurlijk ook alleen gebruikt voor externe toegang. Voor de eigen medewerkers dient ook een maatregel genomen worden.

[15:24] chat1
wordt inzage in dossiers goed gelogd?

[15:25] chat2
Vaak al geïmplementeerd in het ECD

[15:25] chat1
echt waar? ook eenvoudig terug te vinden? en wordt er op gecontroleerd?

Onze ervaring is dat er wel modules te vinden zijn in verschillende pakketten maar dat de reactie van zorginstellingen is dat de mogelijkheden tot monitoring beperkt zijn. Hierdoor blijft de steekproef op een relatief groot gedeelte van de dossiers. Het centraal verzamelen van logging uit verschillende applicaties en het doorzoekbaar maken in het kader van de NEN 7513 zien wij ook veel interesse in daarnaast het realtime monitoren op verdachte benaderingen wordt interessant gevonden.

[15:26] chat2
Nee, niet direct maar het is wel mogelijk bij beveiligingsincidenten.
Je mag medewerkers niet zomaar volgen m.b.t. de logging

[15:26] chat3
het gaat niet om volgen. Controle logging is verplicht, Zie Haga casus.

[15:27] chat1

steeksproefgewijs moet toch kunnen?

[15:27] chat2
Het controleren van de loggings is een reactieve maatregel.
Ik borg dit liever middels het autorisatiebeheer en controle daarvan
Ja dat klopt echter kan je niet alleen vertrouwen op authorisatiebeheer aangezien er ook “zachte” risico’s zijn waar je ook rekening mee moet houden. Een combinatie van goed autorisatiebeheer en een controle van logging.

[15:32] chat1
hoe staat het dan met de NEN 7513 in de sector/bij de leveranciers of zorgorganisaties?
We zien dat in het kader van de NEN 7513 steeds meer levernaciers wel logging aanbieden. Het centraal verzamelen en beheren hiervan is vaak nog niet ingericht. Wij krijgen nog niet veel zelf actief de vraag vanuit zorginstellingen hierover.

[15:33] chat4
De log's tonen in het ECD geeft een sociale controle door anderen en zorgt voor een rem op misbruik.
Dat klopt.

[15:28] chat
Risico's vaststellen; dat zijn er legio ... hoe maak je dit goed inzichtelijk?
Door het doen van een risico analyse, Een ISMS is een centraal punt waar alle documenten rond deze risico’s (beleid, risico’s planning etc) in kunnen worden bijgehouden. Hier zijn verschillende pakketten voor de te koop. Maar we zien ook instellingen met Excel sheets werken.

Pak dreigingsrapporten van Z-cert, NCSC, Verizon, etc erbij. En natuurlijk heb je nog de “technische” risicocategorieën die iedereen wel kent:

- Malware/ Ransomware
- Dataloss
- Disgrunteld Employee
- Availability
- Backup/ Restore
- Vulnerabilities

Overleg daarnaast met alle afdelingen (en zeker ook directie) en vraag waar zij zich zorgen over maken. Maak ook zelf de inschatting welke dingen jij van denkt “dat kan nog wel eens fout gaan”

Dit bij elkaar heb je een redelijk overzicht van risico’s, als je dit in kaart hebt en je hebt maatregelen dan kan je een externe partij een security review laten doen (let op dat deze niet alleen technisch van aard is) waar je dan ook weer risico’s uitkrijgt en zo verder. Dat is eigenlijk de PDCA-cyclus waar we het over gehad hebben.

[15:35] chat
Daarom ook de verwerkersoveenkomst!

[15:37] chat1
je kunt ook een assuranceverklaring vragen. dat geeft zekerheid, die NEN 7510 niet geeft

[15:37] chat
is een PEN test daar niet geschikt voor?

Je kan inderdaad vragen om een pentestbewijs. Soms geven leveranciers een TPM (third party memorandum) af vanuit de pentestpartij. Soms is het ook mogelijk om zelf een test te laten uitvoeren. Dit is afhankelijk van wat voor soort omgeving het is.

[15:42] chat2
onze leverancier van het zorgdossier levert ieder jaar een zgn ISEA 3402 rapportage op

[15:43] chat1
Chat2, onze leverancier van het zorgdossier levert ieder jaar een zgn ISEA 3402 rapportage op en beoordelen jullie die rapportage ook? of neem je hem als kennisgeving aan?
Deze nemen wij aan als kennisgeving.

[15:45] chat2
we hebben nog weinig kennis hoe we dit moeten lezen. Echter organiseert de leverancier (voor corona) een plenaire bijeenkomst met alle klanten die van vragen stellen en vaak ook hun jurist/ controller/ accountant meesturen. Erg leerzaam.

[15:49] chat
Chat1, je kunt ook een assuranceverklaring vragen, dat geeft zekerheid, die NEN 7510 niet geeft Zonder de scope en verklaring van toepasselijkheid zegt een 'NEN 7510 certificatie' van een leverancier mij nog niets
Dat klopt de NEN7510 verklaring moet van toepassing zijn op de volledige dienst die je afneemt. Het is dan ook goed altijd te vragen naar de scope van de verklaring.

[16:02] chat1
We-transfer, Google Drive, Drobbox..... Organisatorische maatregel heel hard nodig!
Dat klopt, daarom goed om er daarna op te monitoren en eventueel bij te sturen.

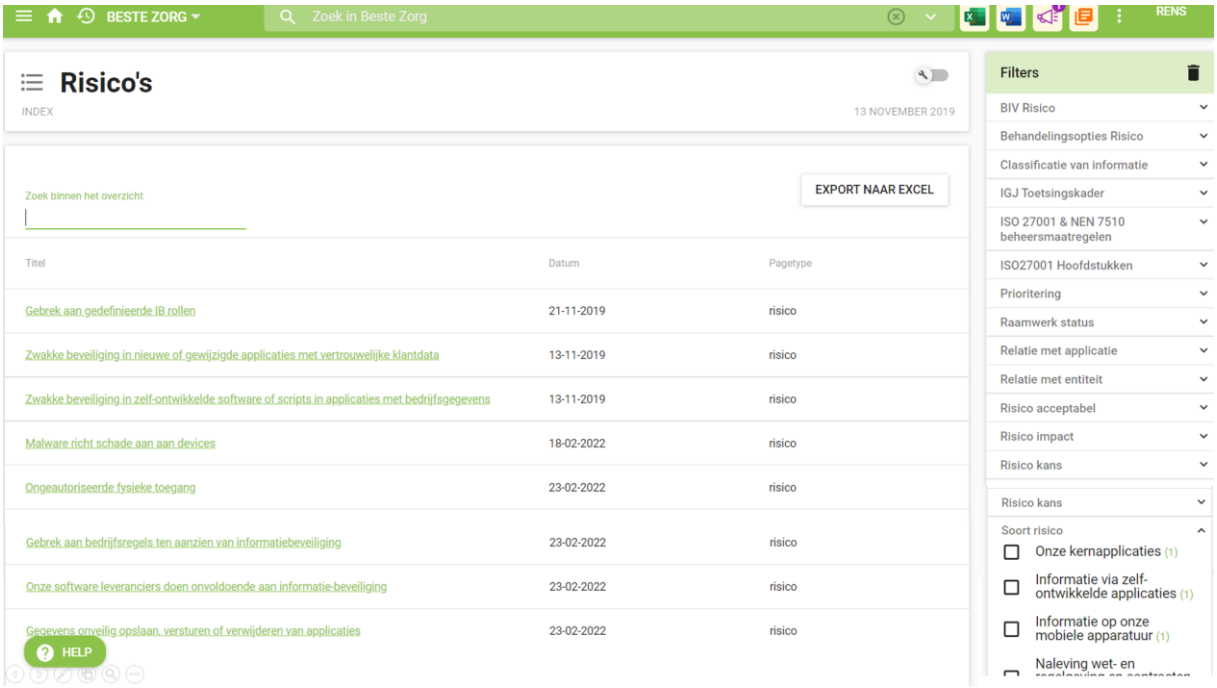
[16:03] chat
Shadow-IT

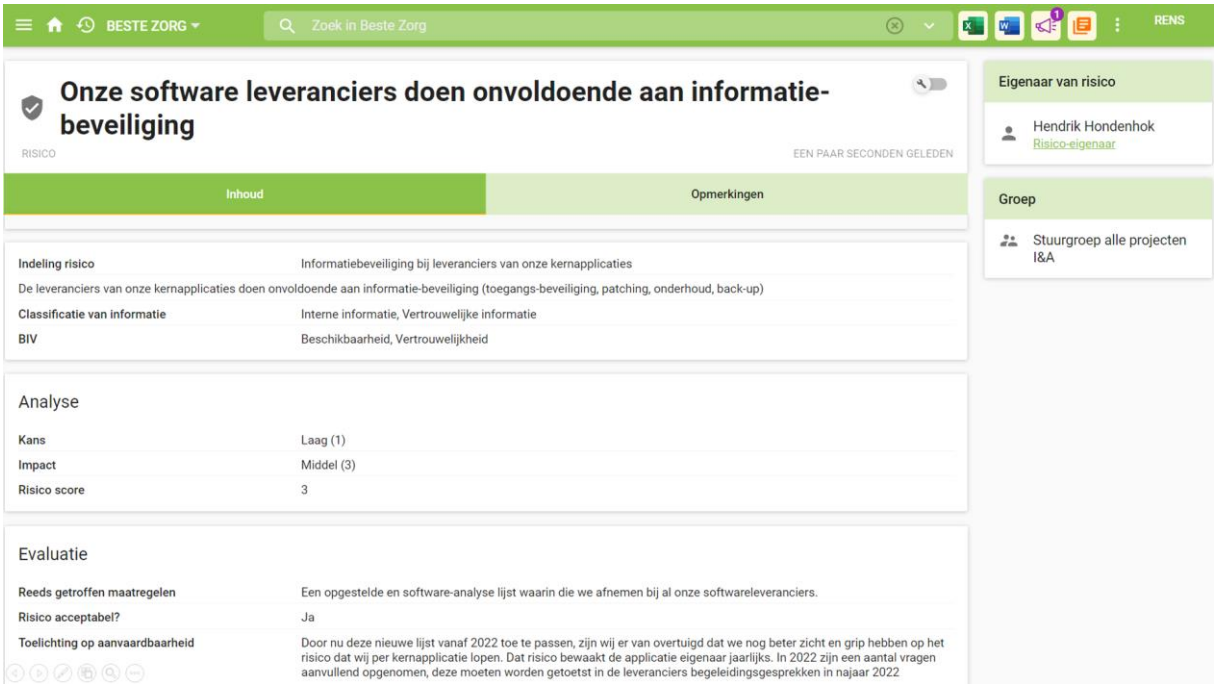
[16:19] chat1
Ik heb een vraag... Ik ben werkzaam als FG in de zorg. Ik ben bekend met de AVG overige privacywetgeving en de sectorale normen. Ik mis echter de technische kennis om bijvoorbeeld een beveiligingsincident als log4j, dat mis ik in praktijk. Hebben jullie een tip voor mij?

[16:21] chat
Een FG adviseert en controleert op het gebied van AVG, zijnde beveiliging van persoonsgegevens. Zorg ervoor dat de FG geen zaken uitvoert op het gebied van security!! Dan ga je je eigen vlees keuren. Dus iemand erbij halen die het weet.

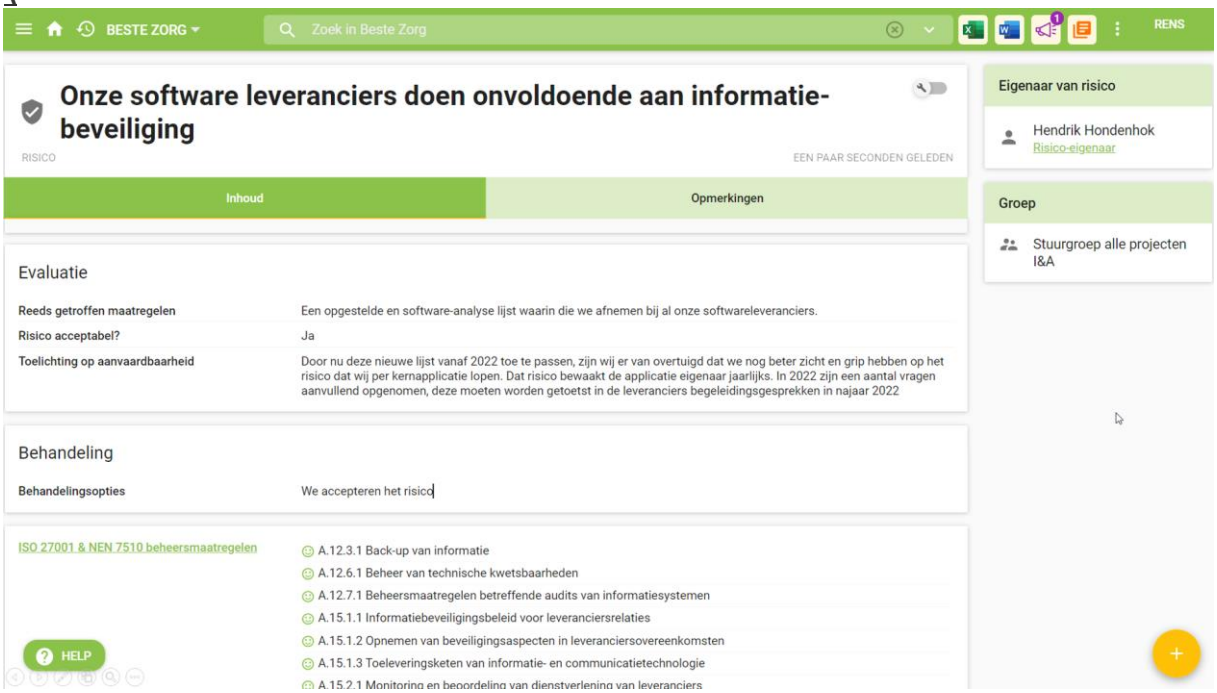
[16:22] chat1
mee eens, het gaat me erom dat ik zou wensen dat ik een beveiligingsincident als log4j kan doorgronden.
Dat klopt, de complexiteit van aanvallen is tegenwoordig groot. Het is niet meer mogelijk zelf alles goed te kunnen doorgronden. Het wordt daarom steeds belangrijker specialistische partijen te verzamelen die als raadgever kunnen dienen.

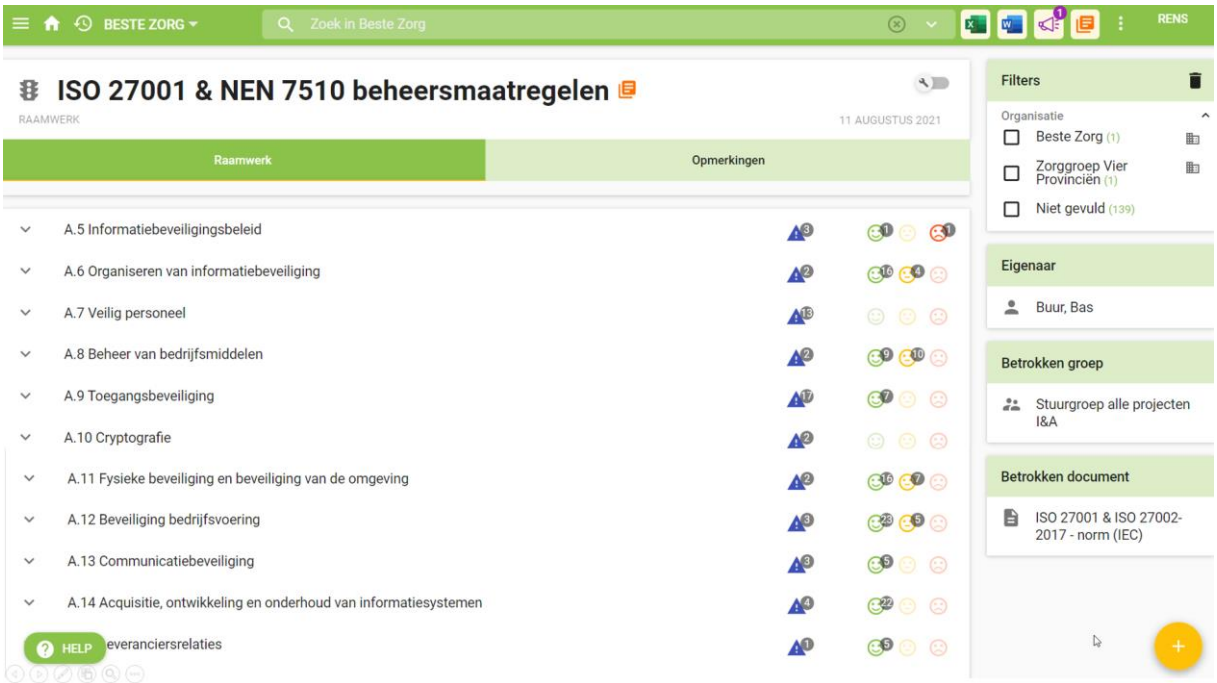
Infozorg presenteerde de volgende informatie





\


BESTE ZORG
Zoek in Beste Zorg
RENS
Onze software leveranciers doen onvoldoende aan informatie-beveiliging
RISICO
EEN PAAR SECONDEN GELEDEN
Inhoud
Opmerkingen
Evaluatie
Reeds getroffen maatregelen
Een opgestelde en software-analyse lijst waarin die we afnemen bij al onze softwareleveranciers.
Risico acceptabel?
Ja
Toelichting op aanvaardbaarheid
Door nu deze nieuwe lijst vanaf 2022 toe te passen, zijn wij er van overtuigd dat we nog beter zicht en grip hebben op het risico dat wij per kernapplicatie lopen. Dat risico bewaakt de applicatie eigenaar jaarlijks. In 2022 zijn een aantal vragen aanvullend opgenomen, deze moeten worden getoetst in de leveranciers begeleidingsgesprekken in najaar 2022
Behandeling
Behandelingsopties
We accepteren het risico
ISO 27001 & NEN 7510 beheersmaatregelen
A.12.3.1 Back-up van informatie
A.12.6.1 Beheer van technische kwetsbaarheden
A.12.7.1 Beheersmaatregelen betreffende audits van informatiesystemen
A.15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties
A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
A.15.1.3 Toeleveringsketen van informatie- en communicatietechnologie
HELP
Eigenaar van risico
Hendrik Hondenhok
Risico-eigenaar
Groep
Stuurgroep alle projecten I&A


BESTE ZORG
Zoek in Beste Zorg
RENS
ISO 27001 & NEN 7510 beheersmaatregelen
RAAMWERK
11 AUGUSTUS 2021
Raamwerk
Opmerkingen
A.5 Informatiebeveiligingsbeleid
A.6 Organiseren van informatiebeveiliging
A.7 Veilig personeel
A.8 Beheer van bedrijfsmiddelen
A.9 Toegangsbeveiliging
A.10 Cryptografie
A.11 Fysieke beveiliging en beveiliging van de omgeving
A.12 Beveiliging bedrijfsvoering
A.13 Communicatiebeveiliging
A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen
HELP
everanciersrelaties
Filters
Organisatie
Beste Zorg (1)
Zorggroep Vier Provinciën (1)
Niet gevuld (139)
Eigenaar
Buur, Bas
Betrokken groep
Stuurgroep alle projecten I&A
Betrokken document
ISO 27001 & ISO 27002-2017 - norm (IEC)