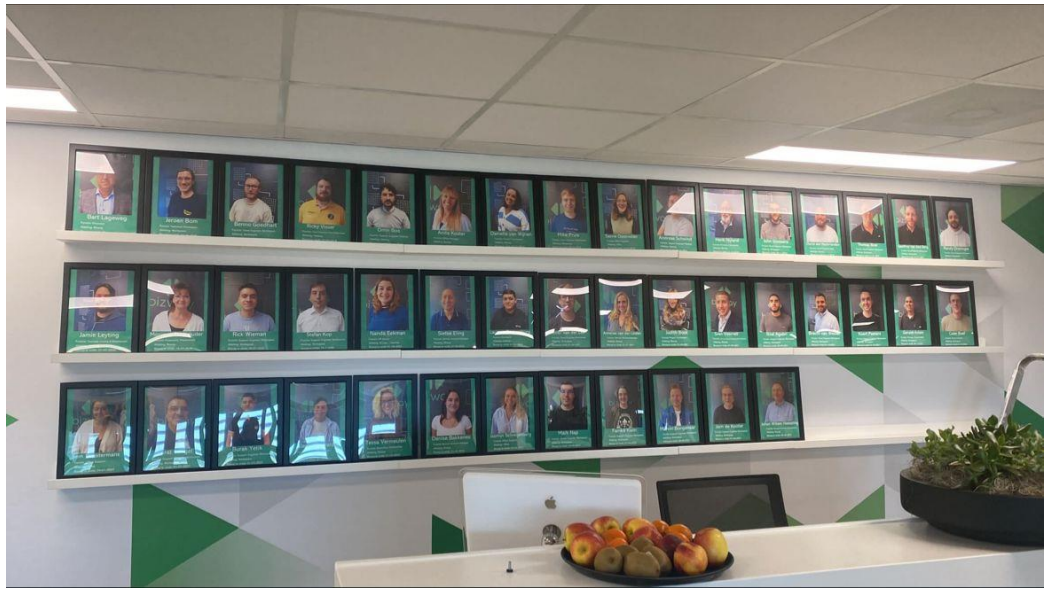
bizway

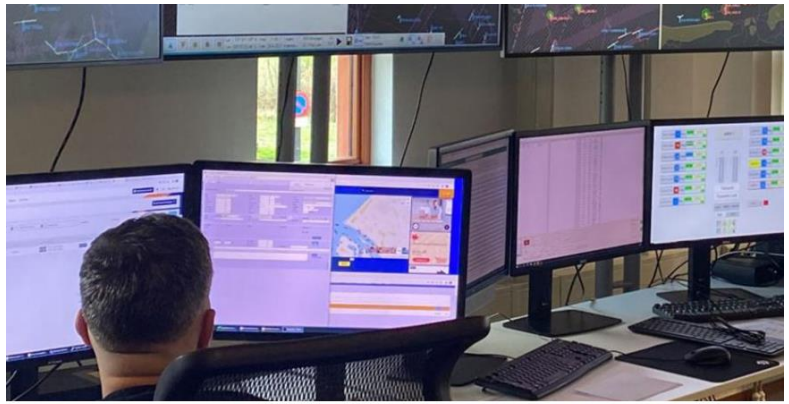
IT partij… met een rugzakje ☺

Bart Lageweg

Founder Bizway BV | CyberHerstel.nl &
Managed hosting & werkplek in de (private)...



Herstel na cyberaanval



Gevaar op zee na hack bij maritieme dienstverlener

Intermax krijgt helft Bizway in handen

14 FEBRUARI 2018 - 09:31 | ACTUEEL | INNOVATIE & TRANSFORMATIE | BIZWAY | INTERMAX GROUP

Christel Dieleman

De Nederlandse Intermax Group verkrijgt de helft van Bizway, specialist in hosting en systeembeheer. Beide bedrijven benadrukken dat het gaat om een gelijkwaardig partnerschap.

'Samenwerken is een must in deze markt', vertelt Bart Lageweg, eigenaar van Bizway. 'Als kleinere partij kun je alleen overleven met een partner waar je je prettig bij voelt. Die partner hebben we in Intermax gevonden. We zetten deze stap zodat we onze kennis kunnen verbreden en vergroten.' De leiding over Bizway blijft in handen van Lageweg. Ook de vestiging in Bodegraven blijft bestaan.

Wie heeft er wel eens een ransomware aanval meegemaakt op zijn omgeving...

Weet iemand waar dit is?

VIDEO: Brand bij oliebedrijf in Dordrecht snel onder controle

Bizway's Cyberherstel aanpak

Calamiteit

Normale operatie	Noodhulp & schade beoordeling	Herstel van kritieke deel operatie	Werkend in herstelmodus	Stabiliseren en opschalen	Normale operatie
	Crisismanagement			Project- & servicemanagement	
	▪ Incident response ▪ Digitaal forensisch onderzoek (schade)	▪ Voorbereiding herstelacties ▪ Uitvoeren herstelacties van kritieke (IT-)functies ▪ Scan, Analyse & Mgt ▪ Gecontroleerd opstarten IT-omgeving en beheren	▪ Zorgen dat kritieke (IT-)functies blijven draaien ▪ Start beheer as-is	▪ Doorvoeren van verbeteringen op gebied van continuïteit en security	▪ DR-plan ▪ Excellente Supportdesk ▪ Managed Werkplek & hosting Services ▪ Pentesten ▪ Security & dossier monitoring ▪ Continue verbeteren
	NFIR	bizway			GUARDIAN 360°
Start	Herstel begint	Herstel gereed	Restauratie	Terug naar normaal	

Aanval of brand/diefstal -> Uit de praktijk ipv mooie plaatjes

- Zorg dat je **NIET** op het netwerk het recovery plan hebt staan, **ELKE KEER** is dit zo!
- Wie heeft regie, en waar staat dat? EN als diegene op vakantie is (of al even niet geslapen heeft), wie dan…
- Als een partij als Bizway je komt helpen, dat doen we graag… wij kennen de omgeving niet.
- Ga geen ruzie zitten maken met je oude partij, alsjeblieft, die hebben de kennis van de omgeving, en slapen vaak deze hersteldagen (en erna) ook niet.
- Bepaal per proces, samen met je IT partij, wat de maximale hersteltijd is, en maximale downtime, als "alles" weg is, dan weten wij namelijk ook de volgorde… dit weet je niet na nachten slapen.
- Geef mensen te eten!!
- Regel hotels, doe niet moeilijk over HR dingen, alles is stuk.. Indien wel, dan doen wij het voor je, en sturen we achteraf de rekening…
- Vergeet het trauma van de mensen niet, dat is echt, heel erg echt, en je zult hier iets mee moeten, mensen zijn voor het leven getekend, of je nou aan de knoppen zit qua besluitvorming van dat ene backup plan wat niet is afgenomen, of dat poortje te veel hebt opengezet…

IT & OT in de keten

Onze klanten zitten allemaal in een keten, niet allemaal NIS2 (veel wel), maar allemaal leveren aan NIS2 partijen..

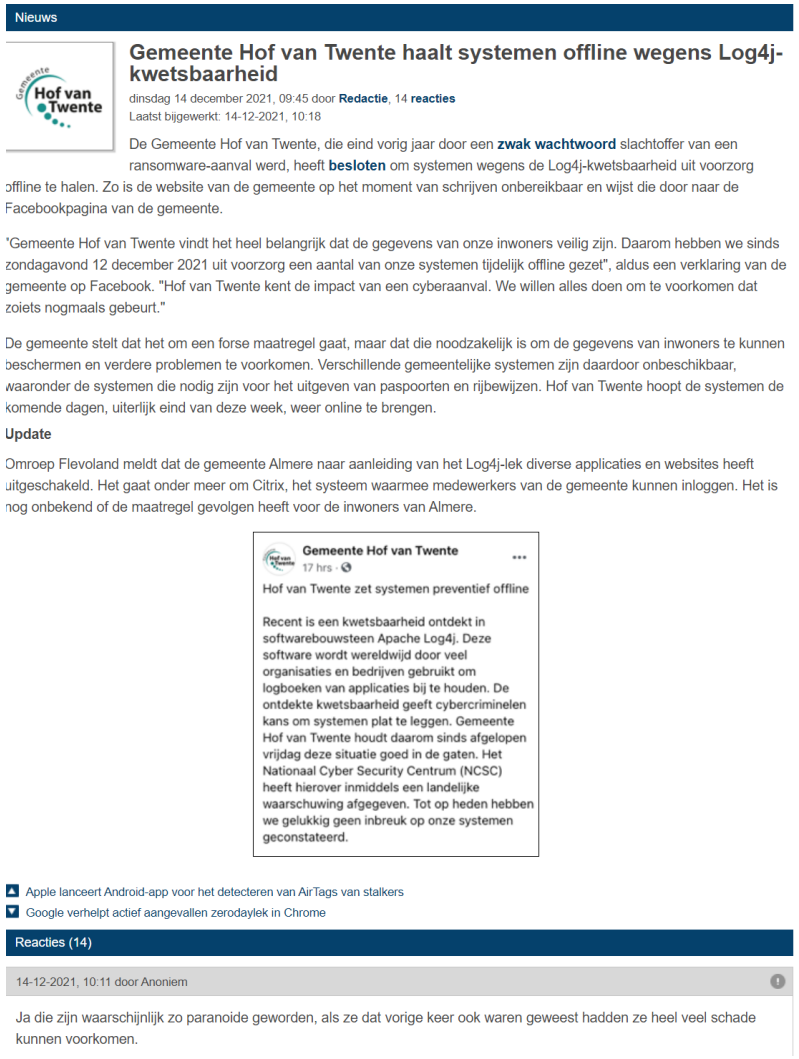
Wie vallen er onder de NIS2

Vitale partijen hebben meer dan 10M omzet en/of meer dan 50 mensen in dienst en vallen onder onderstaande sectoren:

- **Energie:** Energieproducenten, -verdelers en -leveranciers.
- **Transport:** Luchthavens, havens, spoorwegen, busvervoer en andere vervoersystemen.
- **Gezondheidszorg:** Ziekenhuizen, zorginstellingen en andere instellingen die zorg verlenen.
- **Water:** Drinkwaterbedrijven, afvalwaterbedrijven en andere waterbeheerders.
- **Financiën:** Banken, verzekeringsmaatschappijen en andere financiële instellingen.
- **Overheidsdiensten:** Centrale overheid, provincies, gemeenten en andere overheidsorganisaties die essentiële diensten leveren, zoals politie, brandweer en rechtspraak.
- **Digitale infrastructuur:** Provider van internettoegang, hostingproviders en andere digitale aanbieders.

De partijen die leveren aan bovenstaande partijen (keten) moeten hoe belangrijker ze zijn, hoe meer maatregelen ze moeten nemen. Bepaal dat nu ☺ voordat er brieven komen van de NIS2 partijen, of hun accountants.. Of je even wil verklaren dat je er klaar voor bent... Want het antwoord hoeft niet altijd te zijn, we voldoen aan alles, wel dat je er over nagedacht hebt.

Verantwoordelijkheid? Hof van Twente besloot alles uit te zetten



Nieuws

Gemeente Hof van Twente haalt systemen offline wegens Log4j-kwetsbaarheid

dinsdag 14 december 2021, 09:45 door **Redactie**, 14 **reacties**
Laatst bijgewerkt: 14-12-2021, 10:18

De Gemeente Hof van Twente, die eind vorig jaar door een **zwak wachtwoord** slachtoffer van een ransomware-aanval werd, heeft **besloten** om systemen wegens de Log4j-kwetsbaarheid uit voorzorg offline te halen. Zo is de website van de gemeente op het moment van schrijven onbereikbaar en wijst die door naar de Facebookpagina van de gemeente.

"Gemeente Hof van Twente vindt het heel belangrijk dat de gegevens van onze inwoners veilig zijn. Daarom hebben we sinds zondagavond 12 december 2021 uit voorzorg een aantal van onze systemen tijdelijk offline gezet", aldus een verklaring van de gemeente op Facebook. "Hof van Twente kent de impact van een cyberaanval. We willen alles doen om te voorkomen dat zoiets nogmaals gebeurt."

De gemeente stelt dat het om een forse maatregel gaat, maar dat die noodzakelijk is om de gegevens van inwoners te kunnen beschermen en verdere problemen te voorkomen. Verschillende gemeentelijke systemen zijn daardoor onbeschikbaar, waaronder de systemen die nodig zijn voor het uitgeven van paspoorten en rijbewijzen. Hof van Twente hoopt de systemen de komende dagen, uiterlijk eind van deze week, weer online te brengen.

Update

Omroep Flevoland meldt dat de gemeente Almere naar aanleiding van het Log4j-lek diverse applicaties en websites heeft uitgeschakeld. Het gaat onder meer om Citrix, het systeem waarmee medewerkers van de gemeente kunnen inloggen. Het is nog onbekend of de maatregel gevolgen heeft voor de inwoners van Almere.

Gemeente Hof van Twente
17 hrs ·

Hof van Twente zet systemen preventief offline

Recent is een kwetsbaarheid ontdekt in softwarebouwsteen Apache Log4j. Deze software wordt wereldwijd door veel organisaties en bedrijven gebruikt om logboeken van applicaties bij te houden. De ontdekte kwetsbaarheid geeft cybercriminelen kans om systemen plat te leggen. Gemeente Hof van Twente houdt daarom sinds afgelopen vrijdag deze situatie goed in de gaten. Het Nationaal Cyber Security Centrum (NCSC) heeft hierover inmiddels een landelijke waarschuwing afgegeven. Tot op heden hebben we gelukkig geen inbreuk op onze systemen geconstateerd.

Apple lanceert Android-app voor het detecteren van AirTags van stalkers
Google verhelpt actief aangevallen zerodaylek in Chrome

Reacties (14)

14-12-2021, 10:11 door Anoniem

Ja die zijn waarschijnlijk zo paranoide geworden, als ze dat vorige keer ook waren geweest hadden ze heel veel schade kunnen voorkomen.

Wat zegt NIS2

- https://www.digitaltrustcenter.nl/nis2/startpunt

7. Hoe maak je een toeleveringsketen veilig?

" De keten is zo sterk als de zwakste schakel "

Een bekende metafoor die zeker in cybersecurity opgaat. Bedrijven zijn vaak afhankelijk van de (deel)producten of diensten van toeleveranciers. Als bedrijven digitaal met elkaar verbonden zijn, krijgt de afhankelijkheid nog een andere dimensie; een beveiligingslek bij de ene organisatie kan grote gevolgen hebben voor de organisatie waarmee het digitaal verbonden is. Daarom is verlangt de Europese NIS2-richtlijn dat 'belangrijke' en 'essentiële' bedrijven en organisaties maatregelen nemen voor de beveiliging van de toeleveringsketen.

Wat kan er in de keten gebeuren?

Er zijn grote verschillen in digitale weerbaarheid tussen bedrijven, sectoren en ketens. Het kan zijn dat de digitale weerbaarheid van jouw bedrijf op orde is, maar je toch aanzienlijke risico's loopt omdat jouw toeleverancier of (IT-)dienstverlener kwetsbaar is voor cyberrisico's. Dit is een risico voor de beschikbaarheid, de vertrouwelijkheid en de integriteit van je bedrijfsprocessen, informatie en daarmee jouw hele bedrijf.

Er zijn meerdere soorten digitale *supply chain* risico's die jouw bedrijf kunnen aantasten. Deze worden toegelicht aan de hand van een drietal scenario's:

1. Een toeleverancier levert niet meer als gevolg van een digitale aanval;
2. Je (IT-)dienstverlener is gehackt en hierdoor heeft de aanvaller mogelijk ook toegang tot jouw (digitale) systemen;
3. Er is een kritieke kwetsbaarheid ontdekt in één van de (digitale) producten of diensten die je gebruikt in je bedrijfsproces.

Lees over de 'kaashack', de hack die de Rotterdamse haven platlegde en hoe vijf gemeenten in Limburg hun dienstverlening moesten stopzetten na een hack in de keten.

Take a way

- Maak afspraken met je leverancier, wie wat waar, qua verantwoordelijkheid, waar zit je in de keten?
- Maak cases, en simuleer deze, in een soort “war room setting”
- Plan een jaarlijks “hebben we alles onder controle, volgens de keten” meeting in
- BEGIN! Vandaag!, NIS2 100% in orde hebben, dat is geen probleem (wet is er niet), er niets mee doen, is wel onhandig
- Het is geen grapje, persoonlijke aansprakelijkheid van de directie, van iedereen in de keten als je er (echt!) een zooitje van maakt!
- Zorgplicht werkt 2 kanten op, MSPers zijn steeds meer verantwoordelijk, maar als wij zeggen “joh.. Je hebt 15 servers in backup, en die zijn gelukt” en je weet dat je er 23 hebt, dan heb je zelf ook een rol. (Rechters vinden dit vaak ook!)