
think4

Tom Smit

13,5 jaar - IT Bedrijf in Bodegraven

Ondersteunen bedrijven met hun complete IT infrastructuur

MSP – IT bedrijf met 20 collega’s

think4

NIEUWS »

Vertrouwelijke informatie valt in verkeerde handen door onoplettendheid

8 november 2018 - **Het versturen van e-mails gaat bij de gemiddelde Nederlandse kantoormedewerker niet altijd goed. Uit onderzoek van Fellowes blijkt dat bijna de helft van de medewerkers een email naar de verkeerde persoon heeft verstuurd (47 procent).**

60 procent van de werknemers heeft weleens

Het percentage dat een mail heeft ontvangen die voor een ander bestemd was, is nog hoger (60 procent). Niet alleen word
ook v
van r
ontva
heeft

Het datalek bij NMBS Europe is veroorzaakt door een menselijke fout. Dat bevestigt de vervoersmaatschappij na een onderhoud met de Privacycommissie. Het bestand met de gegevens was sinds mei beschikbaar op het internet.

Lees ook: Magnette wil snel rapport over datalek bij NMBS
En: Mogelijk persoonsgegevens van 1,5 miljoen NMBS-klanten gelekt

Na een intern onderzoekt blijkt dat een werknemer op een verkeerde knop heeft geduwd toen hij een bestand wilde leegmaken waarin de gegevens stonden. "Om dat te doen, moest hij de gegevens even op een onbeveiligde server plaatsen. Uiteindelijk zijn die gegevens per ongeluk op die onveilige server blijven staan", legt woordvoerster Nathalie Pierard uit.

Nieuws

Heathrow krijgt boete voor verlies onversleutelde usb-stick

maandag 8 oktober 2018, 14:17 door Redactie, 4 reacties

De Britse luchthaven Heathrow moet een boete van omgerekend 136.000 euro betalen wegens het verlies van een onversleutelde usb-stick met persoonlijke gegevens. Een medewerker van de luchthaven **verloor de usb-stick** vorig jaar, die vervolgens in oktober 2017 door iemand in een bibliotheek werd gevonden.

Datadiefstal bij Budget Energie en NLE: mogelijk 29.000 klanten geraakt

03 december 2019 15:02

Datalekken: jouw gegevens liggen voor het oprapen

19 SEP 2019, 12:23 / UPDATE: 19 SEP 2019, 22:21

---

he
en
ch and w
oing to happen?

After a disgruntled worker leaked the personal
employees, many began legal action against th

Tariq Tahir
h October 2018, 3:12 pm | Updated: 9th October 2018, 3:17 pm

28 november 2019 08:07
Laatste update: 28 november 2019 11:06

14

Cybercriminelen zorgen voor 'ramp' op Universiteit Maastricht

Cyberaanval De Universiteit Maastricht zou losgeld hebben betaald om na een computerhack weer bij bestanden te kunnen waar geen back-up van was.

Wilmer Heck 3 januari 2020 Leestijd 2 minuten

24 oktober 2019 17:19
Laatste update: 25 oktober 2019 09:53

39

Bij verzekeraar Allianz Global Assistance zijn gegevens van in totaal 2,3 miljoen Nederlanders gestolen, laat een woordvoerder van Allianz aan NU.nl weten na berichtgeving van *Amweb* en het *AD*.

Datalek bij Achmea: gegevens duizenden verzekerden op straat

De gegevens van duizenden klanten van Achmea liggen na een hack op straat. Het datalek bij de grootste verzekeraar van Nederland is vermoedelijk ontstaan via een medewerker op een kantoor in Apeldoorn, of via iemand uit de omgeving van deze werknemer.

Binnenlandredactie 12-10-18, 19:00 Laatste update: 20:14

Veeam: menselijke fout oorzaak van datalek met database

zondag 16 september 2018, 08:45 door Redactie, 8 reacties

Een menselijke fout was de oorzaak van een datalek bij softwarebedrijf Veeam waardoor miljoenen records van huidige en potentiële klanten voor iedereen toegankelijk waren, zo heeft het bedrijf zelf bevestigd. Veeam is een bedrijf dat back-up- en datarecovery-oplossingen biedt. Onderzoeker Bob Diachenko ontdekte onlangs via de zoekmachine Shodan een database van het bedrijf die voor iedereen toegankelijk was.

De cijfers

- In 2024 heeft 1 op de 5 bedrijven directe schade geleden
- 85% van de bedrijven ooit slachtoffer
- Totale schade: 10 miljard euro per jaar (NL)
- Gemiddeld €300.000,- per incident

- Wereldwijd: 9,5 biljoen US dollar
- Derde grootste economie
- Groei geschat op ruim 15% per jaar

Bron: CBS | NFO | Cybersecurity Ventures


Cybersecurity, wie zijn probleem?
think4

Cybersecurity is een bedrijfsrisico.

Sterker nog: “het is zelfs geen technisch probleem”

Waar moet je beginnen?

“Je kunt geen beveiliging regelen voor iets waarvan je niet weet dat het kwetsbaar is”

Stap 1: Digitale kroonjuwelen

“Begin klein, maar begin gestructureerd. Een middag risico’s in kaart brengen met het MT is een must”

1. Identificeer alle applicaties
2. Bepaal de data locatie
3. Breng onderlinge relaties in kaart
4. Breng de keten in kaart
    - Wie is mijn leverancier?
    - Wie is verantwoordelijk?
5. Je moet het snappen

Stap 2: Risico’s in kaart

“Alleen met inzicht en overzicht breng je in kaart waar risico’s en kwetsbaarheden zitten”

1. Identificeer dreigingen per onderdeel
2. Weeg en rank risico’s (kans x effect x impact)
3. Wie heeft toegang tot data en waarom
4. Bepaal kwetsbaarheden en maatregelen
    - Bedrijfsproces
    - IT omgeving
    - Mensen

Stap 3: Documenteer je beleid

“Dit hoeft geen boekwerk te zijn, 3-5 pagina’s voor een MKB’er is vaak voldoende”

1. Waar liggen rollen en verantwoordelijkheden
2. Start met een incident & response plan
3. Je toont aan dat je ‘in control’ bent
4. Communiceer beleid en train de organisatie/ collega’s

Stap 4: Implementeer IT maatregelen

DUO SECURITY
eye
VEEAM
splunk>
sosafe
SentinelOne
FORTINET
CROWDSTRIKE
CLOUDFLARE
paloalto NETWORKS
mmox smart
Acronis
GUARDIAN 360°
KASPERSKY lab
Windows Defender
SOPHOS
Barracuda
CISCO SECURE
okta
Microsoft Entra ID
Cove Data Protection
TREND MICRO

Quick Wins

“Niet alles kost direct geld. In samenwerking met IT afdeling of MSP’er kun je morgen starten”

1. Controleer 2FA – multifactor authentication
2. Controleer backup procedures, test deze
3. Beperk rechten ‘least privilege’
4. Systemen update-to-date (steekproef)
5. Gebruik waarvoor betaald is
6. Opgeruimd en netjes

Maatregelen anno 2025

“AI het magische woord, we geen AI inzet in cybersecurity, loopt snel achter”

1. AI wordt gebruikt door aanvallers, maar ook door ons
2. Start met logging en monitoring
3. Geautomatiseerd ingrijpen – 24x7
4. Security Operation Center – SOC

Waar voldoe ik nu aan?

Elke dag een klein beetje beter!

“Voortgang en verbetering gaat geleidelijk en in kleine stappen”

Wat ga jij de komende 72 uur doen?