Berenschot

Mijn organisatie gaat op zwart, wat nu?

Luuk Stadhouders, managing consultant bij Berenschot

20 JUNI 2023

B

Waar ligt voor u de grens tussen een incident en een crisis?

B

Kernbegrippen

Rotterdams staalbedrijf slachtoffer ceo-fraude, buit 11 miljoen

24 februari 2022 14:21
Aangepast: 24 februari 2022 15:14

JewoMetaal in de Rotterdamse haven.

Criminelen hebben bij het Rotterdamse staalbedrijf Jewometaal 11 miljoen euro buitgemaakt met een zogenoemde ceo-fraude. Iemand die zich voordeed als topman van het Duitse moederbedrijf gaf een medewerker met succes de opdracht om de miljoenen over te maken.

tweakers

Zoek naar nieuws

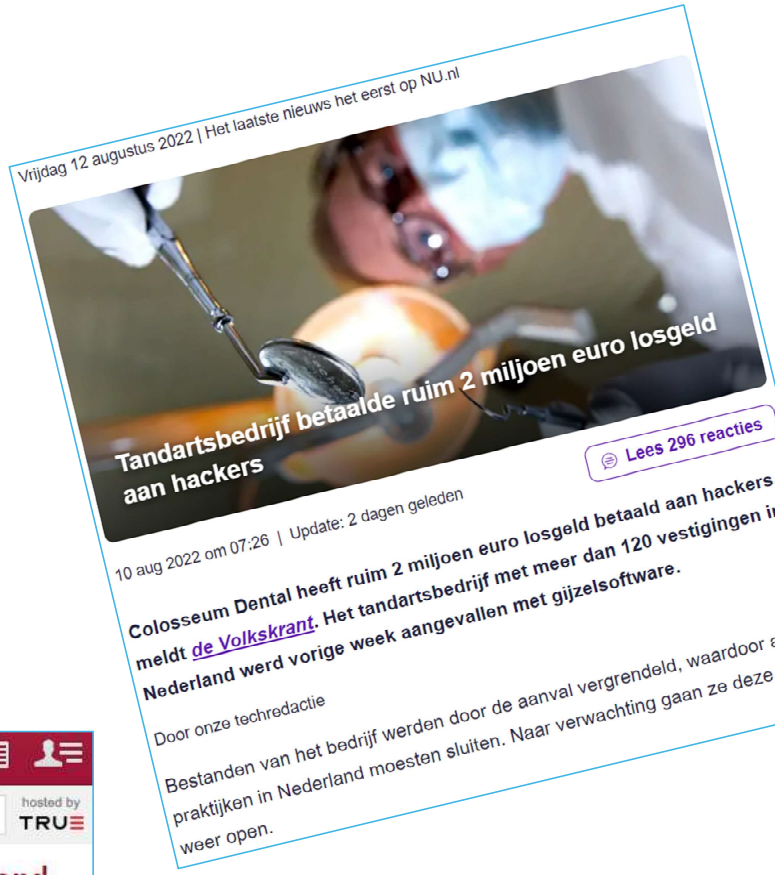
hosted by TRUE

Gegevens van werknemers van voetbalbond KNVB zijn gelekt door 'cyberinbraak'

Door **Tijs Hofmans**
Nieuwscoördinator
Feedback • 04-04-2023 09:18 58

De Koninklijke Nederlandse Voetbalbond is getroffen door een 'cyberinbraak'. Daarbij zijn persoonsgegevens van werknemers gestolen. Over de oorzaak van het lek is nog niets bekend, evenals de omvang ervan.

De KNVB schrijft op zijn website dat er een 'cyberinbraak' heeft plaatsgevonden. Dat gebeurde specifiek bij de KNVB Campus, het opleidingsinstituut van de voetbalorganisatie. De KNVB schrijft in een kort bericht dat er persoonlijke



Vrijdag 12 augustus 2022 | Het laatste nieuws het eerst op NU.nl

Tandartsbedrijf betaalde ruim 2 miljoen euro losgeld aan hackers

Lees 296 reacties

10 aug 2022 om 07:26 | Update: 2 dagen geleden

Colosseum Dental heeft ruim 2 miljoen euro losgeld betaald aan hackers meldt de Volkskrant. Het tandartsbedrijf met meer dan 120 vestigingen in Nederland werd vorige week aangevallen met gijzelsoftware.

Door onze techredactie

Bestanden van het bedrijf werden door de aanval vergrendeld, waardoor praktijken in Nederland moesten sluiten. Naar verwachting gaan ze deze weer open.

B

Citrix

Eind 2019 en begin 2020

- **18-12-2019**: High (kans) / Medium (schade)
- **24-12-2019**: Op basis van nieuwe informatie is de inschaling van dit beveiligingsadvies bijgewerkt naar High/High
- **09-01-2020 (donderdag)**: Actief gescand naar kwetsbare systemen. Nog geen actieve exploit in het wild waargenomen (wordt wel verwacht). Geen patch of fix beschikbaar vanuit Citrix.
- **11-01-2020 (zaterdag)**: Exploit code publiek gemaakt. Geen patch of fix beschikbaar.

B

Een aantal (unieke) kenmerken

- Een ICT-calamiteit kan leiden tot een calamiteit met **fysieke effecten** (bijvoorbeeld uitval (medische) systemen), maar ook een **fysieke oorzaak** hebben (hoogwater leidt tot overlast in datacenter).
- De **snelheid** waarmee een ICT-calamiteit zich manifesteert, is niet te voorspellen. Ook de doorlooptijd laat zich vooraf en gedurende een calamiteit moeilijk inschatten (diverse, nog onzichtbare (mogelijke) oorzaken).
- De **bestrijding** vraagt (1) mogelijk inzet (en afhankelijkheid) van IT met partners, (2) afstemming met of (tijdelijk) alternatieve werkzaamheden door verantwoordelijken van de (primaire) bedrijfsprocessen én (3) effectbestrijding in de (primaire) processen
- **Impact**: Een klein deel van de **bedrijfsvoering** kan geraakt worden of, in het meest extreme geval, tot een totale verstoring van de bedrijfsvoering leiden. ICT-calamiteiten kunnen snel de strategische bedrijfsdoelstellingen van een organisatie raken en grote financiële afwegingen mee gemoeid zijn. Er kunnen gevolgen zijn voor alle bedrijfsprocessen met **maatschappelijke ontwrichting** en/of onrust tot gevolg, m.n. bij een bijzondere samenloop van omstandigheden.
- **Crisisorganisatie** wordt zelf mogelijk ook geraakt in het functioneren door uitval of een beperkte beschikbaarheid van de eigen ICT-middelen (o.a. communicatie).

B

ROC Mondriaan

Augustus 2021

- Een netwerkbeheerder merkt rond 2.30 uur dat er wat mis is met het computersysteem van ROC Mondriaan in Den Haag, een mbo-instelling met 26 scholen.
- Het inderhaast ingeschakelde forensisch IT-bedrijf stelt de volgende ochtend vast dat het echt mis is.
- Hans Schutte, lid van het college van bestuur: '*In eerste instantie hoop je dat de omvang meevalt, maar alles was weg. Dat was een schok. Zelfs de koffieautomaten waren geschakeld aan een systeem*.'

B

Unieke vragen en besluiten

- Betalen van ransomware en/of onderhandelen met criminelen.
- Inschakelen externe expertise: forensische experts, onderhandelings- en digitale expertise, communicatie.
- Uitschakelen (nog niet getroffen) systemen (isolatie), waardoor (delen van) bedrijfsprocessen.
- Geraakte systemen: veilig/integer of niet?
- Crisiscommunicatie over de (dreiging van) aanval of escalatie. Wie voert het woord? Wat deel je?

B

Van wie is (cyber) incident management in een organisatie?

B

Grootste valkuilen

- Onduidelijke criteria ten behoeve van alerteren, informeren en opschalen.
- Lijn versus crisisverantwoordelijkheden lopen door elkaar: in planvorming en ‘in de warme fase’.
- Geen inzicht in kritieke processen en wat te doen als het misgaat.
- Niet leren en evalueren, want ‘*we hebben het toch best oké gedaan*’.
- Niet testen en oefenen…

Luuk Stadhouders MSc CISM

Managing consultant bij Berenschot

l.stadhouders@berenschot.nl
+31 (0)6 2572 2613

Berenschot

Berenschot

www.berenschot.nl

linkedin.com/berenschot