- *Verzorgd door: Sanne Maasakkers (NCSC) en Rob Wassink (DNB)*

- *Doel: Bewustwording van nut en noodzaak van crisismanagementoefeningen*
- *Publiek: Bestuurders, uitoefenaars risk managementfunctie, actuariële functie, actuarissen en andere betrokken personen die betrokken kunnen zijn bij een cybercrisis.*
- *Boodschap: Oefenen van cybercrises maakt uw organisatie aanzienlijk weerbaarder.*
- *Het zorgt ervoor dat de mensen getraind zijn en hun acties tijdens een cyberaanval goed aansluiten op de technische maatregelen en processen die zijn ingeregeld.*

- *Verzekeraars zijn kwetsbaar voor cyberaanvallen. Hoe kunnen zij zich voorbereiden? Is het op orde brengen van de basis(cyber)hyhiene voldoende? Neemt een derde partij alle zorg uit handen, of is het uitbesteden van diensten juist een extra zorg? Naast het op orde brengen en onderhouden van technische maatregelen en processen is het oefenen van processen als incident respons en crisis management van groot belang voor de weerbaarheid van de organisatie.*
- *In deze breakout-sessie gaat u ervaren wat het is als u niet meer kunt vertrouwen op de integriteit van uw klantdata. Moet u onderhandelen en betalen aan de hacker? Hoe het is als u de controle dreigt te verliezen op uw eigen IT-organisatie, en als u zware reputatieschade voorziet …*

DNB

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Crisisgame

Rob Wassink & Sanne Maasakkers

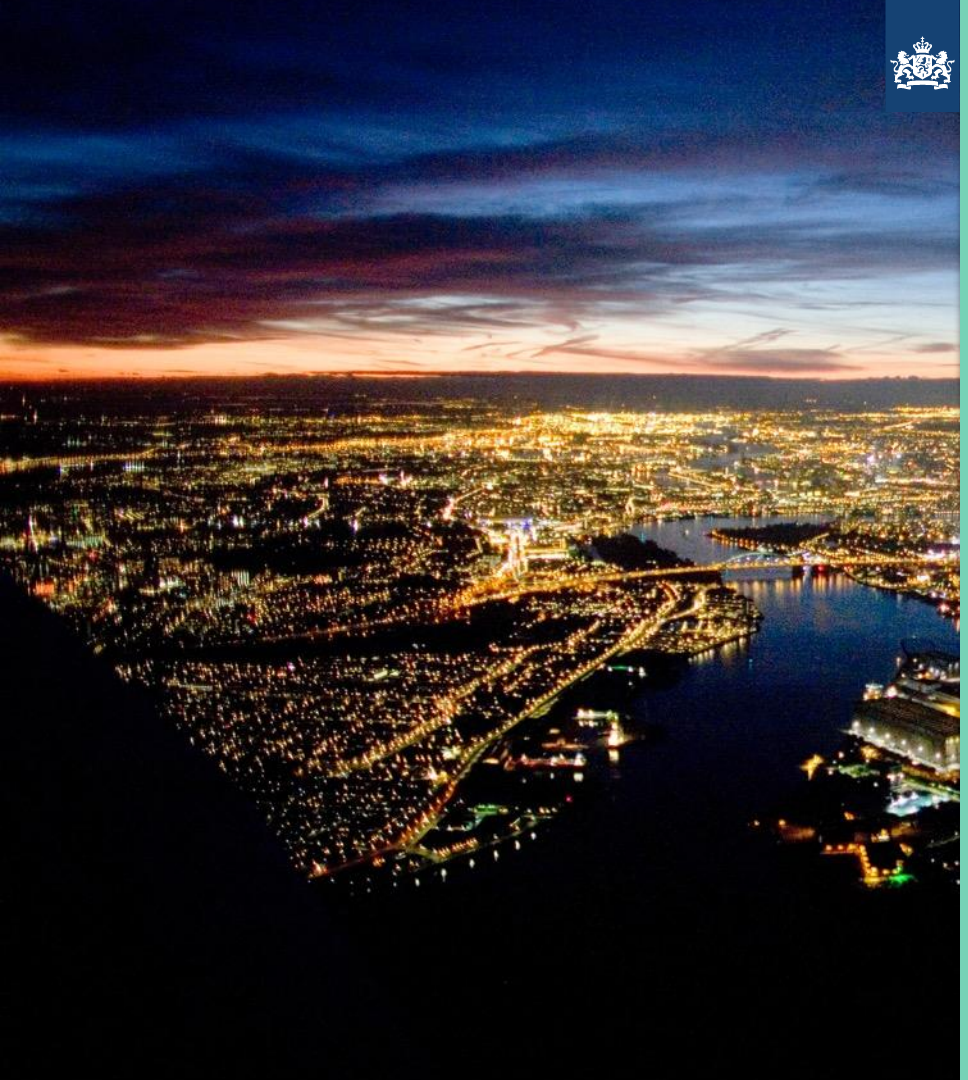
DNB Verzekeringsmiddag, 22 september 2022

Rob Wassink

Cyber security specialist bij DNB

Testmanager TIBER-programma P&V sector

"Focus, discipline and execution with a good laugh"



Sanne Maasakkers

Security specialist bij NCSC

“Het is pas crisis als de koffie op is”

Wie zijn jullie?

- Eindverantwoordelijken en makers van beslissingen tijdens de crisis

We moeten klaar staan voor
*de '**grote cybercrisis**'.*

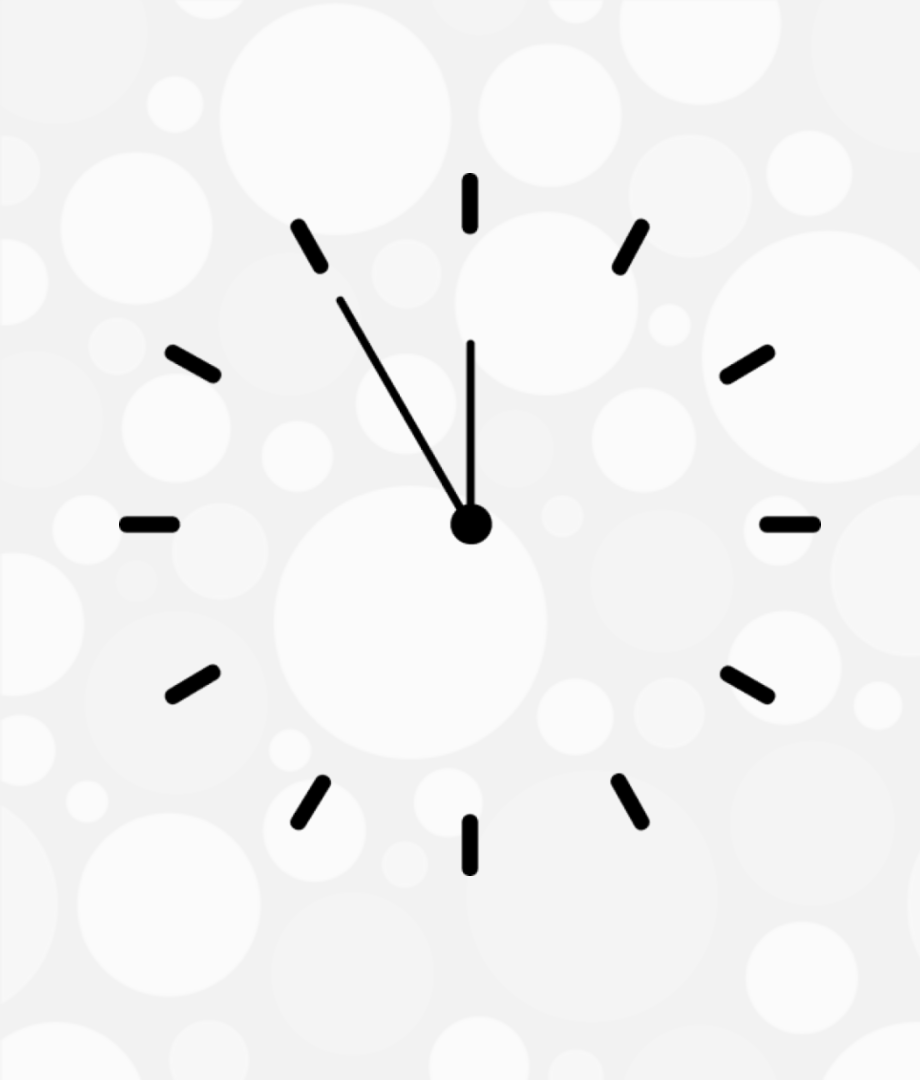
Crisisgame

- Meerdere rondes met nieuwe informatie (injects)
- Op basis van deze informatie moeten jullie een keuze maken

Tool

Yellenge

Deze sessie is interactief en maakt gebruik van Yellenge.



Ronde 1

Dag 1 – 09:30

Meerdere boze meldingen bij klantenservice dat er uitkeringen van levensverzekeringen deze maand niet ontvangen zijn door klanten.

Inmiddels is er ook een verdachte email binnen op het info-emailadres van de organisatie.

We hacked your organisation

C
cyberattack996@proton.me
To info@verzekermij.nl

PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS

We have hacked your insurance company and messed up your customer information

How did this happen?

Our team has found a vulnerability in your network that we were able to exploit. After finding the vulnerability we were able to wander through your internal network and get the highest privileges possible. We are GOD of your internal systems. We were able to mess up with your information. Nothing can be trusted anymore. It's in OUR HANDS.

What does this mean?

We will systematically go through a series of steps of totally damaging your reputation. First, find what we did yourself. You might already got some signals. Next, you will have only have limited time to get in contact with us or we might leak information to internet and press that we have entered your systems and your operation is DONE. Your reputation is damaged and you will have angry customers because of MISSED LIFE INSURANCES.

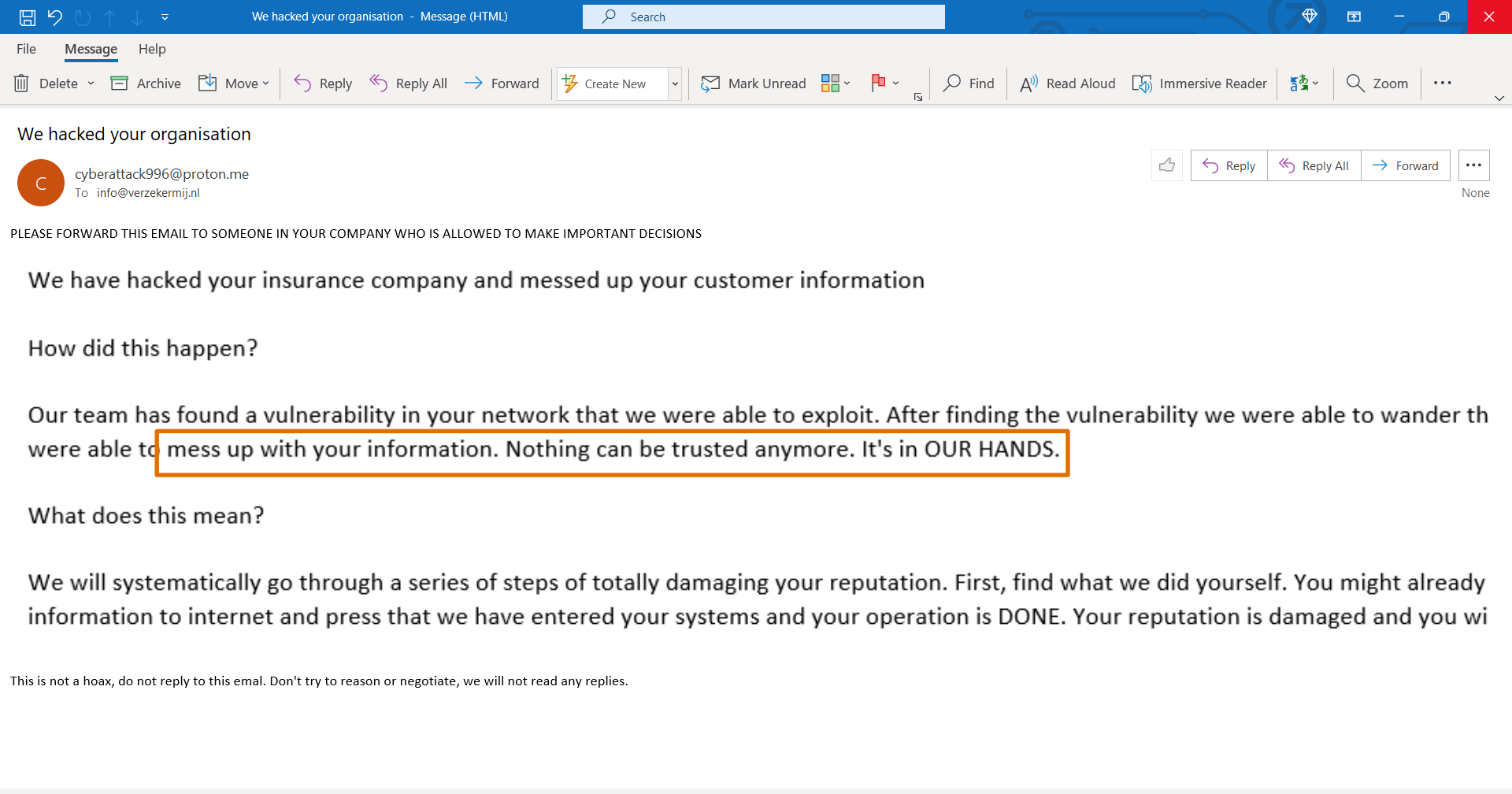
How do I stop this?

We are willing to refrain from destroying your reputation for a fee. Please contact us for the current price and the payment methods.

You can reach us on the following chat URL:
http://skjfjhfaeighepaiherhdbsubfyfroehiehbfief.onion

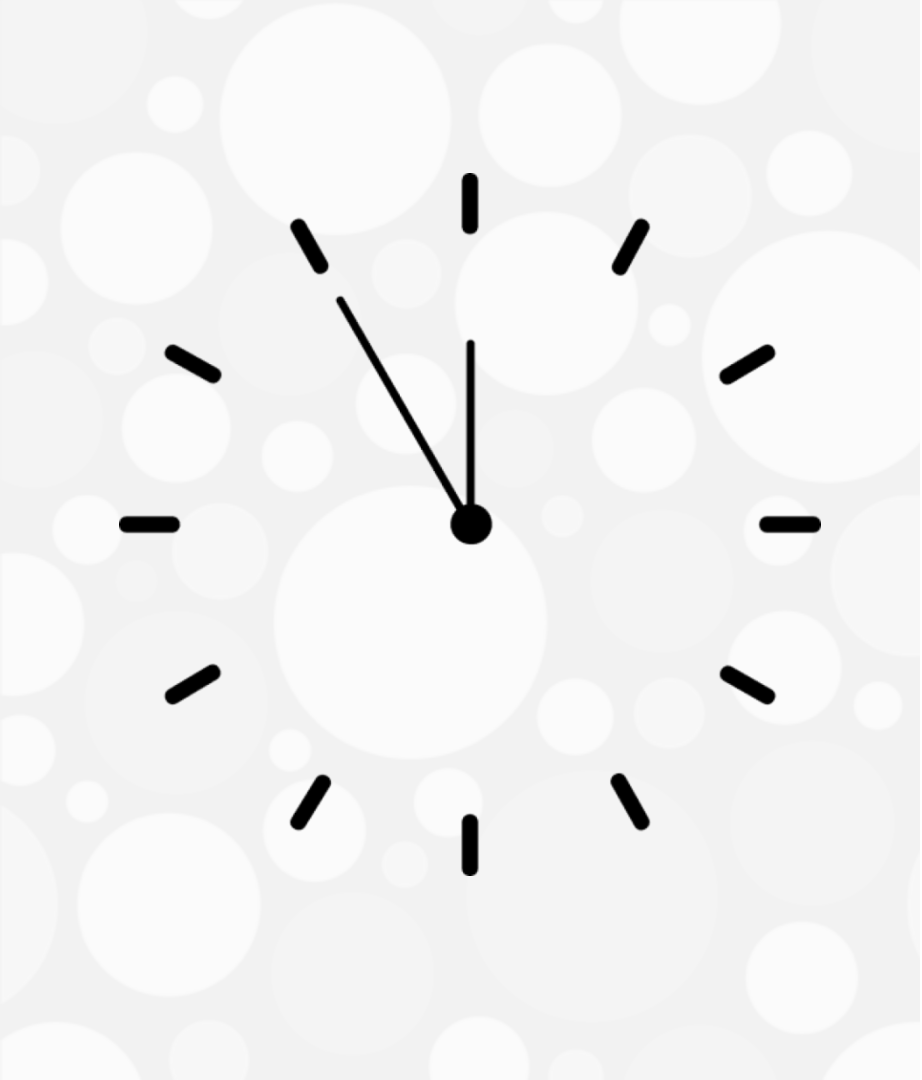
Please mention the following ID to the operator:
623247628573

This is not a hoax, do not reply to this emal. Don't try to reason or negotiate, we will not read any replies.


We hacked your organisation - Message (HTML)
Search
File
Message
Help
Delete
Archive
Move
Reply
Reply All
Forward
Create New
Mark Unread
Find
Read Aloud
Immersive Reader
Zoom
We hacked your organisation
cyberattack996@proton.me
To info@verzekermij.nl
Reply
Reply All
Forward
None
PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS
We have hacked your insurance company and messed up your customer information
How did this happen?
Our team has found a vulnerability in your network that we were able to exploit. After finding the vulnerability we were able to wander th
were able to mess up with your information. Nothing can be trusted anymore. It's in OUR HANDS.
What does this mean?
We will systematically go through a series of steps of totally damaging your reputation. First, find what we did yourself. You might already
information to internet and press that we have entered your systems and your operation is DONE. Your reputation is damaged and you wi
This is not a hoax, do not reply to this emal. Don't try to reason or negotiate, we will not read any replies.
Code: 16 02 90 6

Wie haak je aan in je team?

- Technisch specialisten
- Communicatie
- Legal
- Directie
- HR
- Crisiscoördinatie



Ronde 2

Dag 1 – 14:00

Het crisisteam is bij elkaar gekomen.

Zij zijn begonnen met het veiligstellen van de email, analyseren de afzender van de email en of dit een bekende actor is.

Ronde 2

Dag 1 – 16:00

Onderzoek is gestart met interne specialisten. De afzender blijkt een bekende actor en inderdaad, er zijn onregelmatigheden gevonden in uitbetalings- en administratiesystemen. Mutatiedata in de databases zijn van vorige week. Shodan geeft aan dat de RDP-poort van het internet benaderbaar was.

created_at	updated_at
26-12-19 6:09	4-09-22 5:17
20-04-21 19:37	4-09-22 5:17
26-12-19 6:09	4-09-22 5:17
14-01-20 7:16	4-09-22 5:17
8-09-20 21:22	4-09-22 5:17
8-01-22 15:33	4-09-22 5:17
9-01-22 15:33	4-09-22 5:17
7-06-22 5:45	4-09-22 5:17
25-09-20 21:16	4-09-22 5:17
15-04-19 14:36	4-09-22 5:17
29-06-22 8:49	4-09-22 5:17
10-06-22 8:05	4-09-22 5:17
8-02-20 16:56	4-09-22 5:17
9-02-20 16:56	4-09-22 5:17
4-02-22 1:17	4-09-22 5:17
30-12-20 17:13	4-09-22 5:17
31-12-20 17:13	4-09-22 5:17
20-08-22 18:16	4-09-22 5:17
30-04-22 7:29	4-09-22 5:17
1-05-22 7:29	4-09-22 5:17

35.88.232.153	10:05	3389	closed
35.88.232.153	10:10	3389	closed
35.88.232.153	10:15	3389	closed
35.88.232.153	10:20	3389	closed
35.88.232.153	10:25	3389	closed
35.88.232.153	10:30	3389	closed
35.88.232.153	10:35	3389	closed
35.88.232.153	10:40	3389	closed
35.88.232.153	10:45	3389	closed
35.88.232.153	10:50	3389	closed
35.88.232.153	10:55	3389	closed
35.88.232.153	11:00	3389	closed
35.88.232.153	11:05	3389	open
35.88.232.153	11:10	3389	closed
35.88.232.153	11:15	3389	closed
35.88.232.153	11:20	3389	closed
35.88.232.153	11:25	3389	closed
35.88.232.153	11:30	3389	closed
35.88.232.153	11:35	3389	closed
35.88.232.153	11:40	3389	closed
35.88.232.153	11:45	3389	closed
35.88.232.153	11:50	3389	closed
35.88.232.153	11:55	3389	closed
35.88.232.153	12:00	3389	closed

created_at	updated_at
26-12-19 6:09	4-09-22 5:17
20-04-21 19:37	4-09-22 5:17
26-12-19 6:09	4-09-22 5:17
14-01-20 7:16	4-09-22 5:17
8-09-20 21:22	4-09-22 5:17
8-01-22 15:33	4-09-22 5:17
9-01-22 15:33	4-09-22 5:17
7-06-22 5:45	4-09-22 5:17
25-09-20 21:16	4-09-22 5:17
15-04-19 14:36	
29-06-22 8:49	
10-06-22 8:05	
8-02-20 16:56	
9-02-20 16:56	
4-02-22 1:17	
30-12-20 17:13	
31-12-20 17:13	
20-08-22 18:16	
30-04-22 7:29	4-09-22 5:17
1-05-22 7:29	4-09-22 5:17

35.88.232.153	10:05	3389	closed
35.88.232.153	10:10	3389	closed
35.88.232.153	10:15	3389	closed
35.88.232.153	10:20	3389	closed
35.88.232.153	10:25	3389	closed
35.88.232.153	10:30	3389	closed
35.88.232.153	10:35	3389	closed
35.88.232.153	10:40	3389	closed
35.88.232.153	10:45	3389	closed
35.88.232.153	10:50	3389	closed
35.88.232.153	10:55	3389	closed
35.88.232.153	11:00	3389	closed
	11:05	3389	open
	11:10	3389	closed
	11:15	3389	closed
	11:20	3389	closed
	11:25	3389	closed
	11:30	3389	closed
	11:35	3389	closed
	11:40	3389	closed
	11:45	3389	closed
	11:50	3389	closed
35.88.232.153	11:55	3389	closed
35.88.232.153	12:00	3389	closed

Google cyberattack996@proton.me

https://mandiant.com › blog › known ▾ Vertaal deze pagina

Actor report: APT108

7 mrt. 2022 — APT108 is known for trying to disrupt organisations with national impact, using **cyberattack996@proton.me** as their primary email address for communication..

Wat ga je nu als eerste doen?

Forensisch onderzoekers

Back-ups veiligstellen

Contact opnemen actor

Pers te woord staan

Systemen uitschakelen

Business continueren

Ronde 3

Dag 2 – 13:00

Impact op klanten wordt zichtbaar op social media doordat de hacker informatie over de aanval heeft gedeeld op Twitter en het darkweb. Verschillende mediaplatforms bellen om verhaal te halen, NOS staat voor de deur om een item te maken voor het achtuurjournaal.

NOS Nieuws • Donderdag 22 september, 13:37 •

Verzekeringsmaatschappij gehackt, uitbetalingen onzeker

Een verzekeringsmaatschappij in Nederland lijkt aangevallen te zijn door een hackersgroepering. De hackersgroepering plaatst op Twitter dat zij de maatschappij hebben aangevallen en gegevens niet meer betrouwbaar zijn.

Daarnaast uiten verschillende klanten op social media hun ongenoegen over het voorval: zij zouden last hebben van onjuiste uitbetalingen van onder andere levensverzekeringen.

Een verzekeringsmaatschappij in Nederland lijkt aangevallen te zijn door een hackersgroepering. De hackersgroepering plaatst op Twitter dat zij de maatschappij hebben aangevallen en gegevens niet meer betrouwbaar zijn.

Daarnaast uiten verschillende klanten op social media hun ongenoegen over het voorval: zij zouden last hebben van onjuiste uitbetalingen van onder andere levensverzekeringen.

Daarnaast uiten verschillende klanten op social media hun ongenoegen over het voorval: zij zouden last hebben van onjuiste uitbetalingen van onder andere levensverzekeringen.

Hoe had je deze crisis kunnen voorkomen?

- IR & crisisplan
- Leverancier toetsen
- Red Team-oefening
- ISO-certificering
- Security awareness
- SIEM-dienst afnemen


JOURNAAL

Afronding / wrap up

- Hacker is zonder detectie systemen binnengedrongen via een service die tijdelijk bereikbaar was via het internet door een configuratiefout

- Geen ransomware of datadiefstal, maar integriteit van data staat onder druk. Wie heeft de data?
- Bedenk of je wel of niet moet betalen
- Hoe ga je om met de media en reputatieschade

- Zorg voor een up to date ‘Crisis & incident response-plan’
- Oefen dit plan met regelmaat en neem deel als bestuurder

Meer informatie

- Handreiking oefenen van de cybersecurity alliantie: www.cybersecurityalliantie.nl
- Incidentresponsplan Ransomware van het NCSC: www.ncsc.nl
- TIBER: www.dnb.nl/voor-de-sector/betalingsverkeer/tiber-nl