VNO NCW WEST

⚠ CYBER-INCIDENT: WAT NU?

Eerste-uurkaart | Bewaar fysiek | Lamineer dit kaartje

Als je gehackt bent, heb je mogelijk geen toegang tot digitale bestanden.

1 STOP & BEPERK eerste 15 minuten

- ☐ Raak niet in paniek, maar handel snel
- ☐ Koppel getroffen computers los van het netwerk (kabel eruit, wifi uit)
- ☐ Zet computers **NIET** uit — bewijs blijft zo bewaard
- ☐ Gebruik **GEEN** bedrijfssystemen om te communiceren — gebruik privételefoons
- ☐ Verander nog geen wachtwoorden (je weet nog niet wat gecompromitteerd is)

2 BEL — in deze volgorde eerste 30 minuten

#	Wie	Telefoon	Waarom
1	IT-partner / MSP / Cyber Incident Responder	.....	Zij starten technisch herstel
2	Directie / eigenaar	.....	Beslissingsbevoegdheid
3	Cyberverzekeraar	.....	Vaak 24-72 uur meldtermijn
4	Politie cybercrime: 0900-8844	.....	Aangifte, team cybercrime

3 DOCUMENTEER eerste uur

- ☐ Noteer OP PAPIER: wat is er gebeurd, wanneer ontdekt, door wie, welke systemen?
- ☐ Maak foto's van foutmeldingen op schermen met je privételefoon
- ☐ Raak verder niets aan tot je IT-partner instructies geeft
- ☐ Gooi niets weg en verwijder niets — alles kan bewijs zijn

4 MELD binnen 72 uur verplicht bij datalek

- ☐ Autoriteit Persoonsgegevens — meldplicht datalekken via autoriteitpersoonsgegevens.nl
- ☐ Betrokkenen (klanten/medewerkers) als er risico is voor hun rechten en vrijheden
- ☐ Opdrachtgevers / ketenpartners — check contractuele meldplicht

5 DOORDRAAIEN blijf operationeel

- ☐ Wat kan er handmatig doorgaan? (facturatie, klantcontact, levertijden)
- ☐ Communiceer proactief naar klanten: "We hebben een incident, we zijn ermee bezig"
- ☐ Deel je alternatieve contactnummer (zie achterzijde)
- ☐ Openheid wint het van stilte — klanten accepteren een incident, niet dat je het verzwijgt

Een incident is pas een ramp als je geen plan hebt.

NOODGEGEVENS — VUL DIT NU IN

Invullen, lamineren, en bewaren bij de meterkast, brandblusser of in de bureaula van de directeur

Belangrijkste contacten

Wie	Naam	Telefoonnummer
IT-partner / MSP	.....	.....
Contactpersoon bij MSP	.....	.....
Directeur / eigenaar / Raad van Bestuur	.....	.....
Cyberverzekeraar	.....	.....
Externe incident responder / cyber adviseur	.....	.....
Accountant / boekhouder	.....	.....

Alternatieve communicatie (klanten + personeel)

Alternatief e-mailadres (bv. Gmail, Outlook.com, Soverin)	.....
Alternatief telefoonnummer	.....
WhatsApp- of Signal groep noodcommunicatie	..... aangemaakt? ja / nee
Afgesproken verzamelplaats / belpunt	.....

Kritieke systemen & back-ups

Back-up locatie (waar staan back-ups?)	.....
Laatste back-up test (datum)	.....
Hersteltijd back-up (geschat)	..... uren / dagen
Belangrijkste systeem 1	.....
Belangrijkste systeem 2	.....
Belangrijkste systeem 3	.....
Cloudprovider(s)	.....

Kwartaal-check (elke 3 maanden)

- ☐ Back-up getest? Werkt de restore daadwerkelijk?
- ☐ Zijn er medewerkers vertrokken die nog toegang hebben?
- ☐ Zijn alle systemen en software up-to-date?
- ☐ Is multifactor-authenticatie aan op alle accounts?
- ☐ Klopt dit kaartje nog? Zijn de telefoonnummers actueel?
- ☐ Wanneer is de laatste phishing-test / awareness-sessie geweest?

DRIE DINGEN DIE JE VANDAAG KUNT DOEN:

1. Zet multifactor-authenticatie aan 2. Test je back-up 3. Vul dit kaartje in en lamineer het