Ransomware Noodplan

Voor het MKB — print, hang op, weet wat te doen.

DIRECT HULP NODIG — 24/7

+31 6 11 37 10 19

Van Rosmalen Automatisering · Kraanvogelweg 4, 8263 AA Kampen · KVK 74173278

EERSTE 15 MINUTEN

1. **Isoleer besmette systemen**
   Trek de netwerkkabel eruit en schakel WiFi uit. Voorkom verdere verspreiding via fileshares, VPN en cloud-sync (OneDrive/Dropbox).

2. **Schakel NIET uit**
   Geheugen bevat forensisch bewijs en mogelijk de decryptie-sleutel. Laat systemen aan staan tot een specialist meekijkt.

3. **Bel een ransomware-specialist**
   +31 6 11 37 10 19 — 24/7 bereikbaar. Beschrijf wat je ziet en welke systemen geraakt zijn.

4. **Documenteer alles**
   Maak foto's van het scherm en de ransom note. Noteer tijdstippen, gebruikers en eerste meldingen.

5. **Betaal géén losgeld**
   Politie en NCSC adviseren niet te betalen. Geen garantie op herstel, financiert criminaliteit, vergroot kans op tweede aanval.

CHECKLIST ISOLATIE & ONDERZOEK

- Netwerksegmenten met geraakte hosts afsluiten (VLAN / firewallregel)
- RDP, VPN en remote-toegang van getroffen accounts blokkeren
- Cloud-sessies revoke'en (Microsoft 365: alle tokens intrekken)
- Backups loskoppelen voordat ze ook versleuteld worden
- Logging veiligstellen: firewall, EDR, domain controllers, M365 audit
- Lijst maken van geraakte servers, werkplekken, NAS en VM's
- Indicators of Compromise (IoC's) verzamelen voor forensisch onderzoek

COMMUNICATIE

- Intern: één woordvoerder, korte interne update, geen gokken over de oorzaak
- Klanten / leveranciers: alleen feitelijk informeren wanneer impact bekend is
- Pers: verwijs naar één woordvoerder; geen losse uitspraken
- Personeel: instructies over wachtwoord-reset en MFA

MELDPLICHT & AANGIFTE

AVG / Autoriteit Persoonsgegevens: meld een datalek binnen 72 uur via autoriteitpersoonsgegevens.nl als er persoonsgegevens betrokken kunnen zijn — ook bij twijfel.

Politie: doe aangifte via 0900-8844 of politie.nl. Dit is belangrijk voor verzekering en strafrechtelijk onderzoek.

NCSC / DTC: meld het incident bij het Digital Trust Center (digitaltrustcenter.nl) of NCSC indien van toepassing.

Verzekeraar: informeer je cyberverzekeraar direct — vaak is er een 24/7-loket en eisen ze betrokkenheid bij keuze van incident responder.

BELANGRIJKE CONTACTEN

- Ransomware-specialist (24/7): +31 6 11 37 10 19
- Kantoor Van Rosmalen Automatisering: +31 38 333 61 24
- Politie (aangifte): 0900-8844
- Autoriteit Persoonsgegevens: autoriteitpersoonsgegevens.nl/meldpunt-datalekken
- No More Ransom (decryptie-tools): nomoreransom.org
- Digital Trust Center: digitaltrustcenter.nl

PREVENTIE — VOORKOM DE VOLGENDE AANVAL

- 3-2-1 backup: 3 kopieën, 2 media, 1 offsite/immutable
- MFA op alle accounts (zeker e-mail, VPN, beheer)
- EDR / next-gen antivirus met 24/7 monitoring
- Patchen: OS, hypervisor, firmware en remote-toegang prioriteit
- Netwerksegmentatie en least-privilege rechten
- Phishing-training en geteste incident-response procedure