



Ransomware

Wat is het?

- Ransomware is een malware (kwaadaardige software) die je computer of documenten op je computer versleutelt. Het probeert je te laten betalen om van de blokkade af te komen.

Welke gevolgen heeft het voor jouw bedrijf?

- De bedrijfsvoering kan stil komen te liggen.
- Financiële schade.
- Reputatieschade.
- Zelfs met back-ups kan het enige tijd duren voor de processen van jouw organisatie weer op orde zijn.

Hoe kun je het voorkomen?

- Doe je updates direct.
- Gebruik antivirussoftware
- Open geen e-mails, links, en bijlage(n) van onbekende afzenders.
- Zorg voor een ingebouwde anti-phishing functionaliteit.
- Maak regelmatig back-ups in de cloud of op een harde schijf.

Wat te doen als je te maken hebt met ransomware?

- Betaal niet
- Maak een screenshot van het ransomware bericht. Deze kan je later als bewijsmateriaal gebruiken om aangifte te doen.
- Verbreek de netwerkverbinding.
- Maak een melding bij de IT helpdesk van je organisatie.
- Doe aangifte bij de politie en de Fraudehelpdesk.
- Indien er bestanden zijn geblokkeerd met persoonlijke gegevens, doe dan binnen 72 uur melding bij de Autoriteit persoonsgegevens.
- Kijk op de website van No More Ransom. Hier vind je tools waardoor je weer toegang hebt tot de bestanden op je computer zonder de cybercriminelen te betalen.



Alert Online richt zich op het creëren van bewustwording rondom online veiligheid, op het vergroten van kennis over online veiligheid en op het stimuleren van cybersecure gedrag.

De Alert Online spiekbriefjes zijn gebaseerd op de **cyberspiekbriefjes voor Tweede Kamerleden**.

Kijk voor meer tips en informatie op veiliginternetten.nl